# Information security awareness

## *Local government and Internet service providers*

enisa
European Network and Information Security Agency

# Information security awareness: Local government and Internet service providers

*August 2007*

# Table of Contents

# Summary

This report details the successful information security awareness programmes undertaken by government (national and/or local) with an outreach to Internet service providers (ISPs). These initiatives represent government and ISP efforts to promote and develop a 'culture of security' among users within the European Member States.

It is envisaged that this document will help in disseminating information security awareness good practices and recommendations. This report also offers an opportunity to monitor the progress in national approaches to addressing information security awareness. The report is intended to be used by any public bodies and organisations which are tasked to run initiatives which help end-users learn how to protect information assets proactively.

Because of the limited sample size, the report offers an analysis of the findings and their commonalities without allowing a study of the European trends in this field. The main findings are as follows:

- Information security is seen as a high priority by local government and ISPs;
- The level of knowledge of the target groups is fairly limited or generally low;
- Most of the organisations and public bodies plan, organise and deliver information security awareness initiatives for a period of at least 12 months;
- Within local government organisations, information security awareness-raising activities are often part of a larger ICT campaign;
- Training is considered the most effective technique. Setting out comprehensive computer-based training plans and communication tools can help train employees to ensure programme effectiveness;
- Public–private partnerships can be a highly effective means of delivering campaigns, especially if each organisation can use their respective strengths and mobilise appropriate resources;
- The importance of measuring the effectiveness of information security awareness programmes is duly recognised.

Finally, the report highlights that the current environment still demands the European Network and Information Security Agency (ENISA), the Member States and stakeholder organisations to continue their efforts to positively influence the public's behaviour towards information security, changing the mindset of the human element in order to achieve greater self-awareness.

This study has mainly been compiled on the basis of updates of European countries to the *Information security awareness programmes in the EU — insight and guidance for Member States*. This data has been supplemented by research, interviews and careful study. The research was carried out using a survey which was made available to the European Internet Services Providers Association (EuroISPA)[1], the European Local Authorities' Telematic Network (Elanet)[2], Eurocities[3] and their members.

The analysis and synthesis of data contained within this report are current as of July 2007 and should be read as an interpretation of the information provided.

[1] EuroISPA is the pan-European association of the Internet services providers associations of the countries of the European Union. EuroISPA is the world's largest association of ISPs. Further details are available at http://www.euroispa.org/

[2] Elanet operates under the umbrella of the Council of European Municipalities and Regions (CEMR) focusing on the deployment of information society at regional and local level. Further details are available at http://sed.elanet.org/j/v/839?s=52&v=9&c=692&na=1

[3] Eurocities is a network of major European cities. Further details are available at http://www.eurocities.org/main.php

# Introduction

In 2006, ENISA delivered the *Information security awareness programmes in the EU — insight and guidance for Member States* report as part of its work programme[4] [5]. This document[6] provides an analysis of successful awareness-raising practices adopted by European Member States targeting home users, SMEs, local government, media and ISPs. The 2006 report recognised the need to further elaborate on the involvement of local government and ISPs in the field of information security awareness. As both local government and ISPs play an important role for the continuous progress and use of ICT in Europe, this report offers an overview of recent, successful information security awareness initiatives that government (national and/or local) has undertaken in collaboration with ISPs.

[4] See full text of the *Information security awareness programmes in the EU — insight and guidance for Member States* at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_is_aw_programmes_eu.pdf
[5] Hereafter Information Package 2006.
[6] A CD application is also available.

## *Scope*

The purpose of this report is to provide an overview of recent European awareness programmes targeting local government and ISPs. On this basis, ENISA has created abstracts of the material on awareness-raising initiatives involving local government and ISPs contained within the Information Package 2006. Abstracts sent to the relevant Member States aimed at having the Member States review their 2006 contributions and provide the necessary updates. As the 2006 contributions were related to 14 countries only, research, interviews and careful study have been conducted aimed at gathering further data from all European Member States. To this end, ENISA carried out research using a survey which was made available to the European Internet Services Providers Association (EuroISPA)[7], the European Local Authorities' Telematic Network (Elanet)[8], Eurocities[9] and their members[10].


The analysis and synthesis of data contained within this report are current as of July 2007 and should be read as an interpretation of the information provided. Furthermore, this document should not be seen as a comprehensive source of information of all information security awareness-raising initiatives that have been undertaken or are still ongoing by local government and ISPs; this report is only as comprehensive as the level of details provided by the Member States, organisations and bodies.

[7] EuroISPA is the pan-European association of the Internet services providers associations of the countries of the European Union. EuroISPA is the world's largest association of ISPs. Further details are available at http://www.euroispa.org/

[8] Elanet operates under the umbrella of the Council of European Municipalities and Regions (CEMR) focusing on the deployment of the information society at regional and local level. Further details are available at http://sed.elanet.org/j/v/839?s=52&v=9&c=692&na=1

[9] Eurocities is a network of major European cities. Further details are available at http://www.eurocities.org/main.php

[10] The survey was sent to EuroISPA and Elanet on 20 April 2007. With the support of these two associations the survey was sent to their members.

This document should 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.

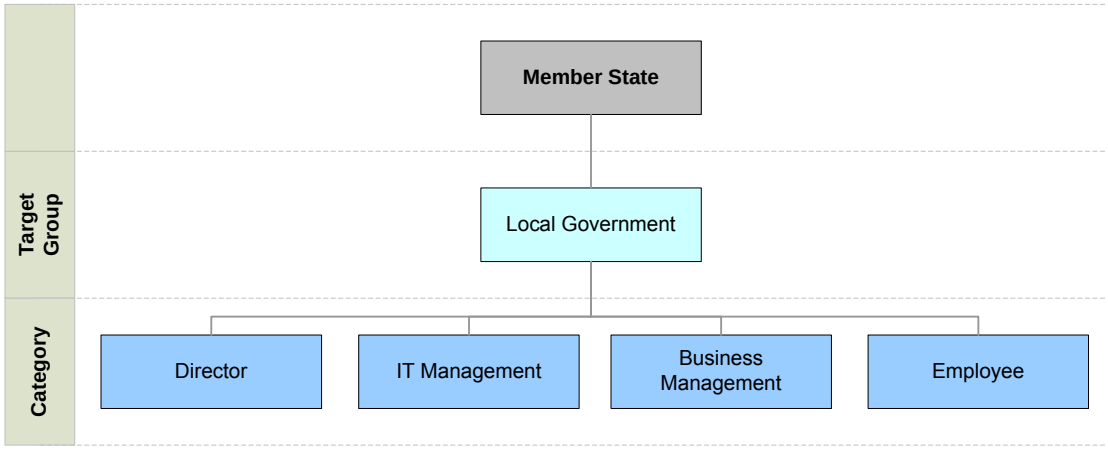
## *Objectives*

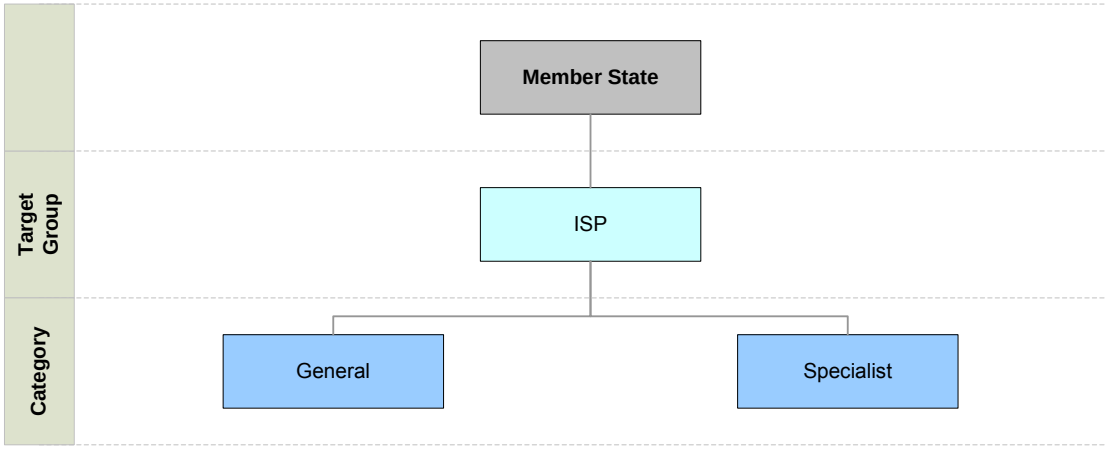
This report is intended to:

- Analyse and help monitor the progress made in national approaches to awareness raising;
- Provide an inventory of good practices from the Member States and other organisations;
- Provide good practice guidelines that can be customised and presented to the Member States to help facilitate their work on awareness raising;
- Contribute to the development of an information security culture in the Member States.

## *Target audience*

This document aims specifically at Member States for use when conducting awareness-raising campaigns. The focus is on two target groups: local government and ISPs. Descriptions on each group can be found in the 'Profile of groups' section. Graphically, these target groups can be illustrated as follows[11]:



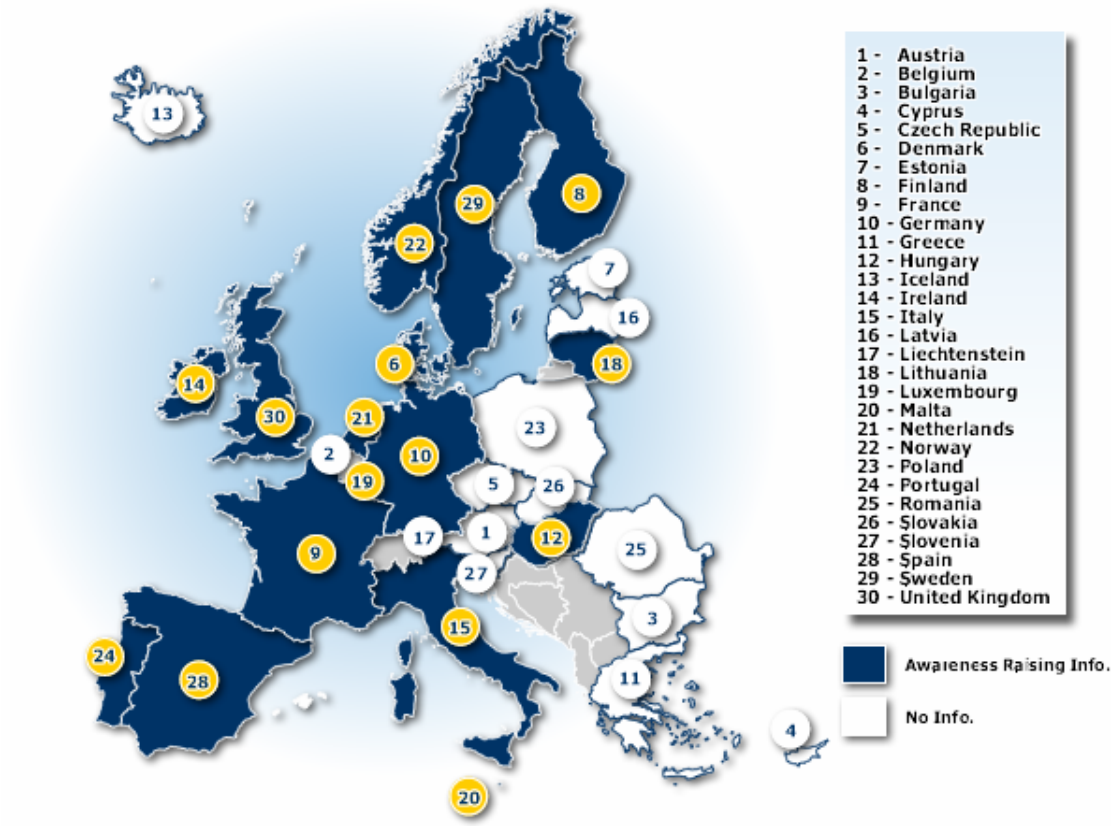

[11] *Information security awareness programmes in the EU — insight and guidance for Member States*, ENISA, September 2006, pp. 13–14. The document is available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_is_aw_programmes_eu.pdf

## *Summary of responses*

The following table indicates which Member State countries provided updates and/or any other additional information to compile this study[12]:

| Country | Required to provide updates to the 2006 Information Package | Provided updates to the 2006 Information Package | Provided some valuable inputs and material for the compilation of the document |
|---|---|---|---|
| Austria | No | - | - |
| Belgium | No | - | - |
| Bulgaria | No | - | - |
| Cyprus | No | - | - |
| Czech Republic | No | - | - |
| Denmark | No | - | Yes |
| Estonia | No | - | - |
| Finland | No | - | Yes |
| France | Yes | Yes | - |
| Germany | Yes | Yes | - |
| Greece | No | - | - |
| Hungary | Yes | Yes | - |
| Ireland | Yes | Yes | Yes |
| Italy | Yes | - | Yes |
| Latvia | No | - | - |
| Lithuania | Yes | Yes | - |
| Luxembourg | Yes | Yes | - |
| Malta | Yes | Yes | - |
| Netherlands | Yes | Yes | - |
| Poland | Yes | - | - |
| Portugal | Yes | Yes | - |
| Romania | No | - | - |
| Slovakia | No | - | - |
| Slovenia | No | - | - |
| Spain | No | - | Yes |
| Sweden | Yes | Yes | Yes |
| United Kingdom | Yes | - | Yes |
| | | | |
| Norway | Yes | Yes | Yes |
| Iceland | No | - | - |
| Liechtenstein | No | - | - |

[12] The abstracts were sent to 14 Member State countries, of which 13 EU members and one EEA member, and to private sector organisations.


1 - Austria
2 - Belgium
3 - Bulgaria
4 - Cyprus
5 - Czech Republic
6 - Denmark
7 - Estonia
8 - Finland
9 - France
10 - Germany
11 - Greece
12 - Hungary
13 - Iceland
14 - Ireland
15 - Italy
16 - Latvia
17 - Liechtenstein
18 - Lithuania
19 - Luxembourg
20 - Malta
21 - Netherlands
22 - Norway
23 - Poland
24 - Portugal
25 - Romania
26 - Slovakia
27 - Slovenia
28 - Spain
29 - Sweden
30 - United Kingdom
Awareness Raising Info.
No Info.

# *About ENISA*

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and the private business and industry actors.

**Contact details:**

For contacting ENISA or for general enquiries on Member State awareness programmes, please use the following details:
e-mail: Isabella Santa, Senior Expert Awareness Raising - awareness@enisa.europa.eu
Internet: http://www.enisa.europa.eu/

# *Acknowledgements*

Several Member States, bodies and organisations contributed directly or indirectly to this work in a number of ways.

The authors wish to acknowledge the efforts of the Member States which provided valuable inputs and material for the compilation of this document.

Additionally, the authors would like to thank the following organisations for the prompt support in the preparation of this report: Galicia e-Commerce Leveraging Centre (CESGA); City of Stockholm; Manchester Digital Development Agency (MDDA), City of Manchester; Oulu municipality, Finland; Örnsköldsvik municipality, Sweden; Aalborg municipality, Denmark; Baerum municipality, Norway; Norwegian Centre for Information Security (NorSIS); Hapsis Education, France; Region of Nordjylland, Denmark; VigiTrust; Vodafone.

Finally, we would like to acknowledge all individuals who contributed to this document with valuable insights, observations and suggestions.

# Profile of groups

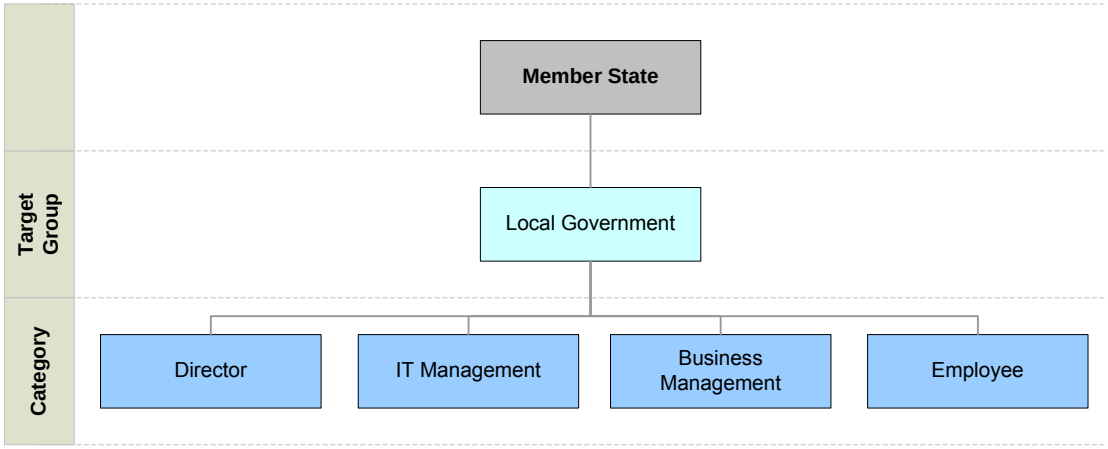
Before detailing the profiles of the two target groups on which this report is focused, it is worthwhile understanding some of the key terms used when describing these groups[13].

| Term | Definition |
|---|---|
| **Target group** | The specific audience that is gtargeted — this is either ISPs or local government. |
| **Category** | The classification or type of target group — for example, a 'director' is a type of 'local government'. |
| **Interest/need** | The main activities which the target group use ICTs to complete — an example would be an adult using 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. |

## *Local government*

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

[13] *Information security awareness programmes in the EU - insight and guidance for Member States*, ENISA, September 2006, pp. 36-38.




## Director

The key decision maker for investment in security.

### Main issues

- Directors are often not realising the potential effects a serious information security breach can have to their organisation. Some examples of the types of threats to security an organisation is typically faced with include:
  - Virus infection and disruptive software
  - Staff misuse of information systems
  - System failures
  - Data corruption
  - Unauthorised access by outsiders, including competitors and hackers
  - Denial of service attacks
  - Disgruntled employees
  - Fraud, theft and deception[14];
- 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 organisations 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;
- In addition, local government users have to face public service compliancy procedures and protocols.

[14] *DTI Information Security Breaches Survey 2004*, DTI, United Kingdom, 2004, available at http://www.pwc.com/uk/eng/ins-sol/publ/dti/dti_technical_report_2004.pdf

**Interests/needs**

- Security framework that is robust and minimises disruptions to business;
- Use of Internet and other ICTs to support business functions and activities;
- Use of ICTs to support job interests including analysis tools, liability issues and organisational operations;
- In addition, local government users need to offer secure and efficient services within the workplace and also when communicating with the public.

## IT management

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

**Main Issues**

- IT Managers or staff can get into the trap of helping to designing and implementing a security framework largely based on IT hardware and software, but can overlook two things: the need for a robust set of policies and procedures and the need for better human behaviour towards security;
- This target group is generally technical in nature however specific messages may be overlooked as being perceived as non-technical or irrelevant or as too technical and aimed at larger organisations;
- Organisations often do not have an information security framework, or if they do it isn't continually monitored or updated. Certain businesses do not have any type of Information Security Management System (ISMS);
- National and International standards such as ISO 17799 and other recognised standards such as COBIT are not being implemented, or if they are then certain controls such as awareness raising or assignment of roles and responsibilities are not being communicated effectively. Monitor and seek improvements controls are also not being implemented sufficiently[15];
- Some of the target group needs to use an Information system security risk management methodology of prevention, detection, response and recovery, but have inadequate controls in place to do so[16].

**Interests/Needs**

- Security framework that is robust and minimises disruptions to business;
- Use of Internet and other ICTs to support business functions and activities;

[15] *Achieving Best Practice in your Business - Information Security: BS 7799 and the Data Protection Act*, DTI, 2004, available at http://www.dti.gov.uk/industries/information_security
[16] *The Management of Security Risks in Information*, Philippe Bouvier, Thales Security Systems, 2004.

- Use of ICTs to support job interests including analysis tools, organisational operations and support manuals.

## Business management

Often not technically orientated, this group of users needs 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.

### 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[17]:
  - Loss of vital information and inability to function
  - Lack of professionalism in eyes of customer
  - Loss of confidential customer information
  - Loss of or compromise in trust and relationship with staff, customers and suppliers
  - Damage to Brand through appearing vulnerable
  - Cost of recovery, repair and management time
  - Cost of disciplinary action
  - Reduced efficiency;
- Management sometimes do not actively support and implement the security policies and procedures within their own business areas;
- In some cases, awareness to staff for their responsibilities as well as security issues in general are not being effectively communicated;
- Information security protection is not seen as an ongoing set of activities but as something that can be implemented once;
- Business Management can face similar issues as to those described in the previous text detailing IT Management.

### Interests/Needs

- Use of Internet and other ICTs to support business functions and activities as well as administration tasks;
- Assurance that information using ICTs is confidential and private

## Employees

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

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

**Main Issues**

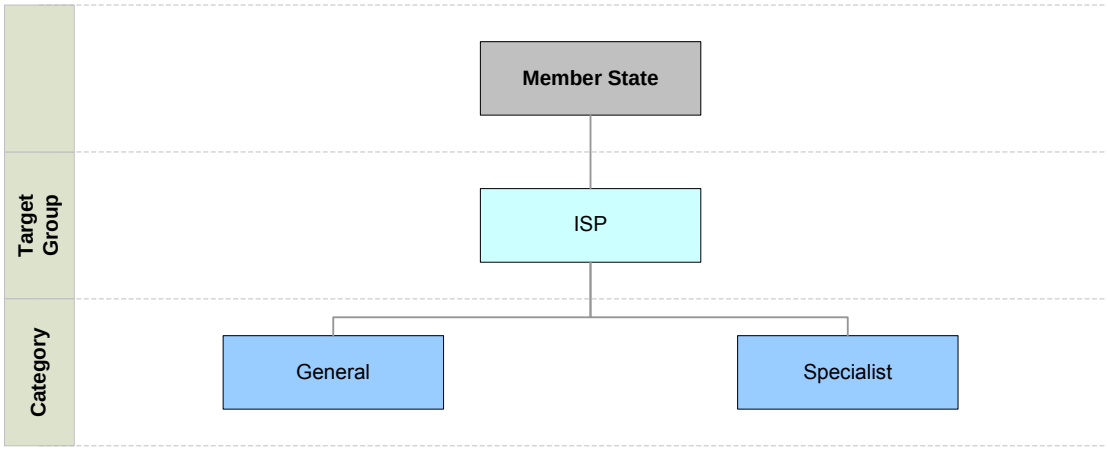
- In the majority of cases, employees want to do the correct thing with respect to information security however they frequently don't know what that is;
- Users should be following clear and documented information security policies and supporting procedures however in a lot of cases they have no clear visibility;
- There is a lack of adequate knowledge as to why security controls are needed and an employees responsibility to adopt them.

**Interests/Needs**

- Using ICTs to perform work related or administration tasks;
- Assurance that any action online is confidential and private.

## *ISPs*

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




### General

This consists of private sector firms that offer a diverse range of products and services; the areas covered are more than just offering an Internet sign-up and connection service. In

addition to a subscription for online access, services may include e-mail, chat, customised web portals, WiFi hotspots or media content such as video or music. The target audience for ISPs comprises both businesses and citizens.

**Main issues**

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

**Interest/needs**

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

## Specialist

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

**Main issues**

- The main issues facing specialist ISPs are similar to those listed in the general ISPs section.

**Interest/needs**

- The interests and needs are similar to those listed in the general ISPs section.

# Good practices by country

The information detailed in the following section correlates to the updates that were received back from the Member States and/or to additional information and material gathered. It is worth noting the following:

- For consistency, the structure of the document is the one used for the Information Package 2006;
- Where there are no updates, the same information published in 2006 has been displayed as still valid;
- Where a section for a specific country does not exist, it is either because no information was supplied by the Member States or because no material has been gathered.

# 1. Denmark

Based upon the supplemented information from research and interviews, the following section for Denmark has been detailed:

Local government as user of information systems

## Local government as user of information systems

### Recent awareness programmes and initiatives

In 2006, the region of Nordjylland, in northern Denmark, started a project called 'IT security in primary schools' aiming at raising information-security awareness among school teachers.

The campaign's main target group were teachers, but the initiative also aimed to target parents and pupils as well. In the first phase of the project, it was decided to pilot the initiative in two schools of Aalborg. A feasibility study was conducted in order to examine the level of IT security competence among teachers and school staff. The study clearly demonstrated a serious lack of both knowledge and accessible material on IT security. As a result of the feasibility study, an e-learning application and information material were developed as a basic tool for piloting the campaign.

Following the pilot, the material has been revised and then distributed to all 37 primary schools in Aalborg.

The main campaign lasted for two weeks and, during that period, teachers were encouraged to discuss and work on the information material. At the end, the teachers had to complete an interactive quiz integrated with an e-learning application. In order to gauge the results between schools, each school received a unique school code, and each school had its own administrator who registered teachers for the quiz. To participate in the quiz, every teacher logged in with his or her email address. Hence, the number of teachers completing the quiz, as well as their individual score, was tracked. The overall score for each school was calculated and the winner received a prize.

The campaign was very well received and even had some attention from the regional TV channel TV2 Nord in October 2006. After having completed the awareness-raising campaign in December 2006, an evaluation report was prepared and sent to the Danish Ministry of Science, Technology and Innovation[18].

The region of Nordjylland in collaboration with the city of Aalborg and the Danish Ministry of Science, Technology and Innovation all contributed to the 'IT security in primary schools' project.

[18] For more information on the importance of measuring the effectiveness of information security awareness programmes see *Information security awareness initiatives: current practices and the measurement of success*, ENISA, July 2007, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf

*It is worthwhile emphasising the need to define the specific audience that is targeted by the awareness programme to better plan and implement the initiative.*

*In Denmark, a study was conducted before the beginning of the campaign demonstrating a serious lack of both knowledge and material on IT security. As a result of the feasibility study, an e-learning application and material was developed as a basic tool for the campaign. It was important to make the message interactive in order to promote security awareness in an effective way.*

*Moreover, after completing the awareness-raising campaign, an evaluation report was prepared and sent to the Danish Ministry of Science, Technology and Innovation. The evaluation of any initiative is essential to understand its effectiveness. Different methods are used to assess the effectiveness of a programme using both quantitative and qualitative approaches. There are four main approaches: process improvement; attack resistance; efficiency and effectiveness; internal protections.*

# 2. Finland

Based upon supplementary information from research and interviews, the following section for Finland has been detailed:

Local government as user of information systems

## Local government as user of information systems

*Recent awareness programmes and initiatives*

In 2006, the city of Oulu created the Competence Oulu 400 project. Some 400 wireless local area network (WLAN) access points have been set up in the city's busiest areas allowing all citizens to surf the Internet free of charge.

The main goal of the Competence Oulu 400 project is to provide the means for the citizens of Oulu to become pioneers in using wireless services — regardless of time and place. The main activities comprise expanding the free and wireless panOULU network (public access network OULU), building a citizens' portal with municipal e-services, participating in the EU 'Wireless cities' project and improving citizens' IT skills by personal training.

Nine citizens' web-trainers offer training to the general public, home users and employees in different public places such as libraries, youth centres, senior service centres and municipal offices. The level of knowledge of the target groups was estimated to be medium. In order to promote the project, the city of Oulu made use of different channels to deliver the message, such as events and theme days, fact sheets and e-newsletters. The city has also joined events organised by others.

The city produced self-study material to support the work of the web-trainers, and this has been published online. The material comprises a number of modules, such as basic computing, mobility, e-services, working wireless and security (online and at home).

The security module offers tips on how to improve information security in everyday life and explains how the Internet and its services can be used in a secure way. Topics covered include:

- Data security, emphasising the importance of secure passwords and the creation of backups of important files;
- Computer virus protection, i.e. information on malicious code and how to protect oneself from being infected;
- Antivirus for mobile phones, a topic that provide instructions on protecting mobile phones from being infected by viruses;
- 'Netiquette' for the Internet, emphasising the rules of correct and polite behaviour among youngsters and parents using the Internet and e-mail correspondence.

In particular, 'netiquette' for the young addresses the following matters:

- 'I have a right to my privacy', urging care when publishing personal information on the Internet;
- 'I have a right to be left alone', informing on the seamy side of Internet anonymity, i.e. everyone should pay attention to the fact that people may not be who they claim to be in chat forums or similar;
- 'I must not be cheated', pointing out the fact that the Internet is filled with inaccurate and even false information, urging young people to evaluate the credibility of information found on the Internet.

The Competence Oulu 400 project started towards the end of 2006 and will end in December 2007.

More information (in Finnish) is available at:
http://oulu.ouka.fi/taito/english.html — to access the web page of the programme
http://oulu.ouka.fi/taito/tietopaketit/ — to get more information on the self-learning material.

# 3. France

Based upon the updates received on the contribution provided last year, the following section for France has been detailed:

Government as partner with civil society

## Government as partner with civil society

### Recent awareness programmes and initiatives

*F@mily online (F@mille en ligne: 'Sur internet, la securité ça commence aussi par vous')*

In May 2006, the French Ministry of the Family launched an information security-awareness campaign informing parents of the potential risks to which minors are exposed while surfing on the Internet and to make them aware on how to use the Internet. As part of the *F@mille en ligne* programme, the ministry broadcast a series of 10 films. These films show the Internet experiments of a family and its knowledge on various existing security solutions. Each 45-second episode was broadcast twice on the two most popular channels for children and young people in France (TF1 and M6) between 15 May and 2 June 2006.

This national information security awareness campaign was intended to develop a constructive and positive dialogue on the use of the Internet within families. The initiative aimed at:

- Informing parents of the potential risks their children may face while surfing on the Internet;
- Making families aware of how to use the Internet.

The key message of the campaign was 'On the Internet, security starts with you'.

*Preliminary studies*

The IFOP polling institute was asked to carry out a survey to compare the knowledge that parents have of the use their children make of the Internet compared with what teenagers declare they do on the Internet.

The survey was developed in two parts: 'Parents and the use of the Internet by their children' and 'Internet usage by teenagers'. This study highlighted, in particular, the following issues:

- 25 % of teenagers declared that they carry out purchases on the Internet, whilst 91 % of the interviewed parents stated that their children never buy on the Internet;
- 42 % of teenagers who have a blog 'never' or 'rarely' speak about it with their parents;
- 38 % of teenagers 'never' or 'rarely' speak with their parents about their activities on the Internet, and 69 % of them estimated that this 'does not interest their parents';

- For 55% of teenagers who know that the home computer is equipped with a parental control access software, 20 % estimated that the software is 'effective but easily avoidable', and 6 % considered the software 'ineffective';
- 36 % of teenagers declared that they have already been confronted more than once to 'shocking, violent or pornographic images or contents on the Internet';
- Only 48 % of them spoke about it with their parents;
- In parallel, a study by the Delegation of the Family indicated that, in February 2006, only 15 % of home Internet connections were equipped with parental access control software;
- Finally, at the end of 2004, a Credoc study stated that, when 75 % of the 11–17-year-olds said they were 'familiar' with the technological environment of the Internet, only 45 % of the parents could say the same.

*Campaign target*

Target groups for the *F@mille en ligne* campaign were: the general public; the parents of children and teenagers surfing the web; and teenagers aged between 11 and 17 years old.

*Concept*

The viewer is watching different members of a family using the Internet. Through their experiments, various topics are approached:

- Personal and banking data protection;
- Blocking of undesirable websites and mail;
- Monitoring the dependence on online games, etc.

The campaign encourages parents to monitor the use that their children make of the Internet.

*Channels used*

- Television (TF1, M6): 45-second film broadcast just before the news;
- Websites of the ministries involved: Family, Industry, National Education, Interior, Justice, Youth and Sports and Prime Minister; banners with campaign logo linked to the Ministry of the Family website;
- Web portals of the private partners: banners with campaign logo linked to their own information page on the campaign.

*Multipliers*

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

*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 a broader audience within the target group. Several partners or multiplier bodies can be used to help deliver the messages as part of an initiative. Examples include: adult education programmes, banks, community centres, industry bodies (unions, associations), ISPs etc.*

*France utilised multipliers such as ISPs to better maximise the reach of the awareness campaign.*

*Impact*

To evaluate the impact of these short movies, a study was carried out by the BVA poll institute which interviewed 1 007 parents. The following results have been gathered:

- 59 % of the parents with an Internet connection at home have heard of, read of or seen an information awareness-raising campaign to inform parents of the potential risks to which minors are exposed while surfing on the Internet and to make them aware of how to use the Internet; 37 % had not heard of the campaign;
- 84 % watched one of the 10 films at least once and declared that they liked them;
- 92 % liked the title and message of the campaign (96 % of the parents have an Internet connection at home);
- 98 % estimated that the films are necessary to raise awareness of information security, 94 % could identify the characters of the films with people they know;
- 71 % indicated that the campaign raised their awareness of the risks encountered while using the Internet.

The campaign was also broadcast on the ISP portals.

*Time frame*

The campaign was announced in September 2006. Some of the activities started immediately afterwards (e.g. procurement, design, shooting) to be able to broadcast the initiative before

summer 2006 and be online with the related projects (i.e. delivery of the parental access control software in April and launching of the family label in September/October). It took eight months to develop the campaign.

*Budget*

The campaign budget is EUR 1 million (limited for the ministry to the realisation and broadcasting of movies), plus the cost of website banners for the ministries and the ISPs.

*Summary of the 10 short movies*[19]

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


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

**Campaign advice/software functionalities: definition of the profiles 'children', 'teens', 'adult'**

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


Chloé uses instant messaging. Someone unknown wishes to be added to her list of contacts and sends her a message. Her mother warns her 'On the Internet it is like in the street, you don't talk to strangers'

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

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

[19] Further details are available at the following address http://www.famille.gouv.fr/protec_enfance/


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

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

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


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

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

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


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

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

Episode 6: *L'achat en ligne* (buying online) http://www.premier-ministre.gouv.fr/IMG/mpg/ep_6.mpg


Chloé, the little sister, wants to buy something on the Internet. She asks for a credit card from her mother. They discuss it.

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

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


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

**Campaign advice/software functionalities: possibility of deciding what information to communicate; prohibition of certain personal details**

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


Yann has just created an e-mail address for his grandmother. She worries about spam. Her grandson activates an anti-spam function.

**Campaign advice/software functionalities: anti-spam function**

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


Chloé chats with a schoolmate she hardly knows. He asks her to send him pictures of her in a swimsuit. She is worried and tells her mother, who explains the risks of such behaviour.

**Campaign advice/software functionalities: blocking of personal data; do not send personal pictures to a stranger**.

Episode 10: *La Dépendance au jeu* (Being hooked on games)
http://www.premier-ministre.gouv.fr/IMG/mpg/ep_10.mpg


Yann is playing his favourite game and his girl friend Malika is not able to drag him away. Malika thinks he is spending too much time in front of the screen, but the time has flown by for Yann.

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

**Public–private partnership**

*Agreement between the Ministry of the Family and ISPs*

On 16 November 2005, following the Conference on the Family, an agreement between the Ministry of the Family, the ISPs (including AOL, Orange (France Telecom/Wanadoo), Alice/Telecom Italia, Noos-Numéricable, Club Internet/T-Online, Neuf Cegetel etc.), and the family and child welfare associations was signed.

Darty Box signed the agreement in February 2007. Free has not yet signed the agreement, but has committed to implement the recommendations by September 2007.

With the exceptions of Darty Box and Free, the agreement is effective from April 2006.

It has been estimated that 30–40 % of users will benefit from this agreement by September 2007.

*ISP commitments*

The ISPs committed to propose free parental access control software to their subscribers offering three different profiles: 'children', 'teenager' and 'adult'.

Each profile has an open or restricted Internet access according to the group who is accessing the Internet. Adults do not have any restriction; teenagers have access to all sites with the exception of those listed on a blacklist or clearly not suitable for this age group; children can only access a set of sites listed on a white list.

E-enfance (e-childhood), an association dealing with child protection on the Internet, carries out surveys directly from the ISP portals in order to check whether ISPs are respecting the agreement.

*Charter between the Ministry of the Family and mobile phone operators*

On 10 January 2006, the association of the French mobile operators (AFOM), the mobile operators Orange (France Telecom/Wanadoo), SFR and Bouygues Telecom signed a charter developed in collaboration with the Ministry of the Family.

*Mobile phone operator commitments*

Mobile phone operators agreed to provide a parental access control device in a systematic and free way to any new mobile phone subscribers from November 2006. Moreover, between April and October 2006, the current mobile phone subscribers received three messages introducing the new safety service.

*L'Internet plus sûr, on se mobilise!* ('The safer Internet, mobilise yourself!')

From 6 to 13 June 2006 as part of the project Confiance[20], the Délégation aux Usages de l'Internet (DUI), Microsoft France and some French ISPs [21] together with the French government joined up to launch the second edition of the national computer security week.


[20] Further details are available at http://www.saferinternet.org/ww/en/pub/insafe/focus/france.htm
[21] MSN France, Maxicours.com, Mindscape and PayPal among others ISPs participated to the initiative.

The nationwide awareness-raising campaign was aimed at raising general public attention to information security matters. The name of the awareness-raising campaign is *L'Internet plus sûr, on se mobilise!* ('The safer Internet, mobilise yourself!').

The main goal of the campaign is to teach Internet users the simple and necessary measures to be taken in order to ensure the security of their computers. The campaign's website recommends and clearly explains five key measures:

- Have an updated antivirus protection;
- Install a parental control tool;
- Activate the function 'automatic update' in Windows;
- Install a fire wall;
- Install software to combat unwanted software such as spyware and malware.


From the campaign's website, it is possible to:

- Download teaching material;
- Test your knowledge of different security topics through quizzes and games;
- Download a security guide presenting the principal threats and risks when browsing the Internet as well as clear instructions on how to avoid these threats and risks;
- Make inquiries on good practice when surfing the Internet.

Moreover, other channels have been used to deliver the message of the campaign, such as guides, stickers, newsletters, magazines and cartoons.

Some figures:

- In February 2006, 26 million people in France regularly went online;
- Out of the 10 million French parents who have at least one child aged between six and 15 years old:
  - 87% believe that surfing is dangerous for children;

- one in three parents (having the Internet at home) does not know the existence of computer protection software;
- 75 % of Internet users are afraid to make online purchases[22].

More information and material on the campaign are available at www.protegetonordi.com

*With the abundance of online information and with time often a premium asset, using channels such as brochures, leaflets and fact sheets etc. are very effective in getting attention and hence raising awareness.*

[22] Further details are available at http://www.internet.gouv.fr/informations/information/statistiques/ and http://dinm.typepad.com/an_net_07_mediametrie/cration_et_consommation_de_contenus_numriques/index.html

# 4. Germany

Based upon the updates received on the contribution provided last year, the following sections for Germany have been detailed:

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

National government as user of information systems

Local government as user of information systems

Government as partner with business and industry

Government as partner with civil society

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

*National awareness-raising strategy*

IT security is an integral part of Germany's national security strategy. The federal government's activities focus on a framework of different aspects related to information security where awareness raising is covered as an essential issue. At the Federal Ministry of the Interior, the federal government has adapted the structures necessary with a view to the complex requirements of information and communication technology at a very early stage.

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

*Responsibilities of the federal government for IT security*

The Federal Ministry of the Interior (BMI), particularly its IT Staff Unit (Office of the Chief Information Officer), are responsible for IT security in the federal government. The German Federal Office for Information Security (BSI) belongs to the area of competence of the Federal Ministry of the Interior.

*The German Federal Office for Information Security (BSI)*

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

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

The work of the Federal Office for Information Security currently focuses on a range of topics, including, for example:

- Critical information infrastructures;
- The Cert-Bund computer emergency response team;
- Early warning systems;
- Fostering citizen awareness for IT security issues;

- Internet security;
- IT security management (IT-Grundschutz);
- Malicious programs;
- Trusted computing;
- Development of cryptographic methods and products;
- Certification and further development of the common criteria;
- Secure e-government;
- Electronic signature;
- Biometrics.

*The national plan for information infrastructure protection*

The growing importance of information infrastructures requires joint action by the State, the economy and society. With the national plan for information infrastructure protection (NPSI), the federal government ensures that these tasks are fulfilled.

To ensure full protection of information infrastructures in Germany, the federal government has set out three strategic objectives in the NPSI:

- Prevention: protecting information infrastructures adequately;
- Preparedness: responding effectively to IT security incidents;
- Sustainability: enhancing German competence in IT security and setting international standards.

The concretisation of these objectives will be done by the implementation plan for the federal administration (Umsetzungsplan Bund) and the implementation plan for critical infrastructures (Umsetzungsplan Kritis), which will be finished in 2007.

*IT security in the federal administration*

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

This plan outlines technical, organisational and procedural standards for security and security management, which the federal ministries will apply in a flexible manner under their own responsibility.

As the national authority in charge of IT security and as the federal government's main IT security service provider, the BSI supports considerably the development of the implementation plan for the federal administration and will assist its realisation. To enable the BSI to fulfil this task, the number of its staff has been and to some extent still will be increased and priorities will be redefined; overall, the BSI will be assigned a more active role as an IT security advising institution.

*Cooperation between the federal government and the private sector*

In Germany, the majority of critical infrastructures are operated by private companies. Therefore, the federal government calls upon its partners in the private sector to take an active part in implementing the NPSI. Together with operators of critical infrastructures, the federal government is preparing the CIP implementation plan (Umsetzungsplan Kritis). It will contain a summary of state-of-the-art IT security measures and supplementary recommendations, in particular with attention to interdependencies to raise the level of IT security in critical infrastructures. The BSI, as well as other competent public authorities, will offer their expertise in assisting the operators of critical infrastructures in implementing the recommendations pointed out in the CIP implementation plan.

*Citizens and society as a whole*

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

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

The aim of the federal government is to encourage people to make more intensive use of existing information and provide recommendations. By following the government's recommendations, citizens actively contribute to IT security in Germany. At the same time, manufacturers and distributors of IT products and services are encouraged to give utmost priority to the security of their products, even at the development stage, and to adequately inform their customers of IT risks and possible protective measures.

*Awareness-raising as a fundamental issue for IT security*

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

*Raising awareness of risks related to IT use*

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

*Use of safe IT products and secure IT systems*

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

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

*Creating framework conditions and guidelines*

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

Each federal ministry will make sure that standards and guidelines are implemented in accordance with the Umsetzungsplan Bund by its own ministry and all authorities within its remit, for example by putting the necessary structures in place.

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

*Identifying, registering and evaluating incidents*

The IT crisis response centre at the BSI, which is currently being put in place, will play the role of a national control and analysis centre that will be able to provide a reliable assessment of the current IT security situation in Germany at any time and that will cooperate with other existing national and international crisis centres in a given incident. To enable the BSI to fulfil this function, a network of sensors will be put in place to detect IT security incidents.

Additional sources supplying information on IT incidents will be made available to the BSI by extending the international watch and warning network, of which the federal government was a founding member. All these measures will ensure that those in charge in the public and to some extent the private business sectors have the information necessary to quickly decide what action has to be taken and can be taken.

*Informing, alerting and warning*

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

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

*IT security competence in school education and professional training*

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

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

# National government as user of information systems

### Recent awareness programmes and initiatives

Refer to the 'Government as developer' and 'Government as partner (business)' sections for information.

# Local government as user of information systems

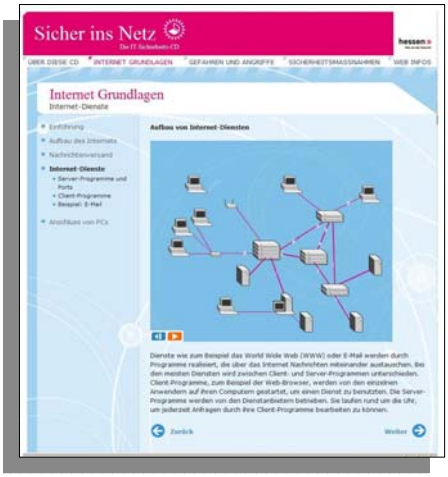
### Recent awareness programmes and initiatives

*Federal State of Hessen*

The Federal State of Hessen, together with Deutsche Telekom, has developed a CD-based training course that aims at educating target groups on how to use IT systems in a secure manner and promoting them within business organisations, private homes and public sector. The training course describes different security problems and gives advice on how to solve them while working with online services.


The main purpose of the 'Safe on the Net' initiative is to explain to the end-users how to deal with IT applications, simple security tools and methods. The training has been developed for users who are not familiar with terms such as 'TCP/IP' and 'http protocol'. The course starts with a basic 'Competence check' that aims at giving an indication of the user's IT security knowledge level. The check is comprised of eight questions covering topics as Internet in general, communication technologies, threats, advices and measures on how preventing such threats. Based on the answers, the user is assigned to one of the following categories: beginner, advanced or professional. For each category a number of training sessions are identified:

1. Basic tour
2. Internet basics
3. Threats and attacks
4. Security measures and
5. Black hat corporation (a test module)




The first training, the Basic tour, gives an overview of the Internet and its security aspects. The trainings 2-4

explain different topics with informative pieces of text and animation. These sessions address a large number of subjects, such as viruses and worms, spam, Internet banking and shopping, firewalls and password security. The last session, Black hat corporation, is a quiz aimed at assessing the user's knowledge from participating in the training.

The training course targets a wide range of PC-users from non-IT specialists, home users, school pupils and students as well as users working in small and medium enterprises.

The initiative got an extensive TV and media coverage. The CD-based training has been as well distributed for free outside the federal State of Hessen and used by Deutsche Telekom to inform their customers and employees. Since July 2005, 20000 copies of the CD have been printed and distributed. To meet the demand, further 10000 copies of the training material will be printed by December 2007.

The Safe on the Net' is only available in German. An on-line version is available at: http://www.hessen-it.de/sicher_ins_netz/inhalte/Ueber/Einleitung/index.html

Refer as well to the 'Government as developer' and 'Government as partner (business)' sections for further information on local government initiatives.

## Government as partner with business and industry

### Recent awareness programmes and initiatives

*Information and guidance provided by BSI*

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

Regarding the publications of the Federal Office for Information Security, the following issues are worth highlighting:

- IT-Grundschutz Manual / IT-Grundschutz Tool / IT-Grundschutz Guidelines / sample guidelines;
- e-government manual;
- Secure use of telecommunications equipment.

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

Brochures used include:

- Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte (wireless local communication systems and related security aspects);
- GSM-Mobilfunk — Gefährdungen und Sicherheitsmaßnahmen (GSM mobile communications — threats and security measures);
- Bluetooth — threats and security measures;
- IT-Sicherheit *Kompakt* (concise guide to IT security).

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

Study results and publications:

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

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

*Some further initiatives which deserve special mention*

*IT-Grundschutz*

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

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

The implementation of the recommendations summarised in the IT-Grundschutz is, in a broader sense, also a precondition for systems with high and highest protection needs. The IT-Grundschutz tool (GS tool) offered supports the development of a security concept. In 2005, IT-Grundschutz was modified to align with the standard ISO/IEC 27001.

Since 2003, the Federal Office for Information Security has been offering a certification system according to the IT-Grundschutz regime which enables the verification of the IT security level actually achieved. In 2006, it was changed to issue ISO 27001 certificates in

compliance with IT-Grundschutz. More than 130 auditors for ISO 27000 audits in compliance with IT-Grundschutz have meanwhile been licensed by the Federal Office for Information Security and are now capable of auditing on-site the implementation of ISO 27001 with an additional examination of technical and organisational safeguards according to IT-Grundschutz. Refer to http://www.bsi.bund.de/english/index.htm (English).

The IT-Grundschutz Manual is supplemented by IT security guidelines — these guidelines give a concise and generally understandable overview of the most important IT security measures. The guidelines focus on organisational measures and on practical examples in order to highlight threats. Refer to http://www.bsi.bund.de/english/gshb/guidelines/index.htm (English).

In view of a strong demand for exemplary IT security concepts, sample guidelines and examples of concepts were published and examples of profiles for small, medium and large enterprises were given.

http://www.bsi.bund.de/gshb/deutsch/hilfmi/musterrichtlinien/index.htm (German)
http://www.bsi.bund.de/gshb/deutsch/hilfmi/beispielprofile.htm (German)

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

Target groups include not just e-government coordinators and decision-makers at federal government, federal-state government and municipal administration levels, but also developers of e-government solutions and interested citizens. The manual covers issues such as ‘secure Internet presence’, ‘barrier-free e-government’, ‘encryption and signature’ together with ‘data-protection compliant e-government’.

*IT security guideline*

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

*Information on security and encryption*

The *IT security — Made in Germany — best practice in secure business processes* brochure was first published in 2004 in cooperation with TeleTrusT Deutschland e.V. and addresses

experts in the fields of IT security and encryption. An updated version of the brochure was published in 2006.

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

The updated issue of the brochure was presented at the ISSE 2006 in Rome. For more information, refer to www.teletrust.de

*Information for business*

In 2003, the Federal Ministry of Economics and Labour (BMWA) and the Federal Ministry of the Interior initiated the establishment of a 'cert' for small and medium-sized enterprises (Mcert) as a public–private partnership, an endeavour including several important partners from the German IT industry.

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

*TeleTrusT Deutschland e.V.*

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

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

*Public–private partnership initiative D21*

Initiative D21 is Germany's largest public–private partnership with more than 400 representatives from industry, associations, political parties, political institutions and other organisations committed to improving the framework for a quick and successful change in the

information and knowledge society in order to boost Germany's international competitiveness and to better equip the country for the future. For more information, refer to www.initiatived21.de

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

## Government as partner with civil society

### Recent awareness programmes and initiatives

Particularly successful initiatives are the awareness campaigns (as detailed in the 'Government as developer' and 'Government as partner (business)' sections) launched by the Federal Office for Information Security together with the security manuals and guidelines that also apply for the more informed public and which have contributed significantly towards enhancing the overall level of IT security in Germany.

The BSI also provides a range of material to inform private users with less or almost no IT security knowledge on the necessity to deal with the topic of IT security in their 'private life'. It also provides tools to support users. Among them, there are two best practice examples in awareness-raising especially worth mentioning:

- www.bsi-fuer-buerger.de: (BSI für Bürger — Federal Office for Information Security for Citizens). The website for private PC users was implemented in 2003 and informs private users on all issues concerning IT security. It is written in an easy-to-understand language, so the non-professional is able to understand and use the tips and checklists provided. Free tools, such as anti-virus protection, personal firewall etc. can also be downloaded from the website. The information offered on the website is distributed through various channels to millions of users. It is also distributed on a CD-ROM, for instance at trade fairs or such events. Cooperation with big companies has been established to use BSI material for awareness-raising among their employees and therefore a broader audience can be reached at relatively low cost. Also part of the portal is a service hotline where citizens can address their questions on IT security by phone, fax or e-mail;

- Bürger-Cert
  Until now the services provided by private certs have only been available to companies, and those provided by the BSI's federal computer emergency response

team, Cert-Bund, have only been available to the public authorities. As such, the Bürger-Cert represents a new approach in Germany, providing impartial and free warnings and information on IT security to the general public and small companies for the first time. Given the palpable need for action, Internet users now have access to a rapid, competent and comprehensive source of information and advice on specific risks and threats resulting from security loopholes on the Internet.

The Bürger-Cert provides its warning and information service in parallel on three different levels. These can be selected by the user entirely in accordance with his or her individual security requirements. The online newsletter *Sicher Informiert* is a fortnightly bulletin covering the main items of security news. *Extraausgaben* (extra issues) of the online newsletter are published in the event of extremely time-critical security loopholes calling for immediate action. Rounding out the service, the *Technische Warnungen* (technical warnings), containing detailed background information, cater for the more technically-minded and more experienced users.

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

Refer to the ‘Government as partner (business)’ section for information on other German initiatives.

# 5. Hungary

Since the publication of the Information Package 2006, no further government initiatives have been undertaken in Hungary by local government and ISPs to raise information security awareness among users. Thus, the following sections for Hungary are still valid:

Local government as user of information systems
Government as partner with business and industry

In the second half of 2007, the currently ongoing national development programmes will kick-off new initiatives.

## Local government as user of information systems

### Recent awareness programmes and initiatives

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

## Government as partner with business and industry

### Internet service providers (ISPs)

ISPs have a great responsibility in creating awareness among users. They have their own association (www.iszt.hu/iszt/English) to represent their interest with policymakers. The first step to raising awareness on a common basis with the government is to be self-regulated. The organisation to coordinate communication between government and ISPs is Hun-Cert, the industry and ISPs' cert of Hungary.

As of now, there have been no joint awareness programmes aimed at the public. Cert-Hungary and Hun-Cert have a good working relationship. They have carried out an exercise to check on how ISPs cooperate in the field of IT security. The results are expected to be communicated through different channels, targeting specialised media as well as the general public later during this year.

### Public–private partnership

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

The eSec.hu consortium is a successful public–private partnership (PPP) aimed at raising information security awareness. The members of the group hold a wide range of IT security spectrum, and are committed to creating a secure IT environment both in the public and private sector. The cutting edge solutions are used by government, public administration, academia, commercial companies, as well as by general public users.

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

# 6. Ireland

Based upon the updates received on the contribution provided last year and on the supplemented information from research and interviews, the following section for Ireland has been detailed:

Government as partner with business and industry

# Government as partner with business and industry

### Public–private partnerships

#### MakeITsecure.ie

The Department of Communication, Marine and Natural Resources together with BT, Dell, Eircom, the Irish Bankers Federation, IAB, Microsoft, Symantec, the National Centre for Technology in Education, Ward Solutions and Vodafone are working together to raise awareness of the urgent need for consumers and businesses to make their computer secure [23]. This public–private consortium has created the second national computer security awareness campaign: 'makeITsecure'[24]. The growth in PC ownership and availability to children, the increased use of online banking, the increased volume of spam, Internet access and usage and the current broadband levels of over 15 % of the population are some of the reasons why the consortium has launched the second edition of this initiative. The 2005/06 campaign addresses new and emerging issues, such as: phishing; identity theft; spyware; and child safety online.

The 2005/06 initiative is:

- Liaising with Northern Ireland;
- Having a TV advertising campaign;
- Focusing on consumer campaign and child safety;
- Increasing the number of groups participating.

The makeITsecure.ie website provides guidance and top tips on how best to protect end-users' personal information[25]. The following goals have been achieved so far:

- Awareness increased to 44 % (from 33 % in 2004);
- Security measures taken by Internet users all increased;
- Over half of 'aware' users undertook extra PC security measures as a result of the campaign;

[23] Since the previous editions of the campaign, new partners have joined the consortium.
[24] Detailed information on makeITsecure national computer security awareness campaign is available at: http://www.makeitsecure.ie/home.asp.
[25] Top tips are available at: http://www.makeitsecure.ie/topTips.asp

- Understanding of terms such as ‘identity theft’ and ‘spyware’ improved dramatically in the post-2005 campaign research with scores of 55 % (from 24 % pre-campaign) and 49 % respectively (from 19 %).

As the ongoing need to educate end-users has been recognised, another campaign will be launched in 2007 building on the brand of makeITsecure. Two main themes will be discussed: securing your computer and safe use of your computer. Particular emphasis will be given to child safety, inviting experts to participate in the initiative. As in the previous editions, TV will be used as the main channel to disseminate the messages of the campaign. A budget of over EUR 1.5m has been estimated.

*Public–private partnerships can be a highly effective way to deliver campaigns, especially if each organisation can leverage strengths and resources.*

*In Ireland, the Department of Communication, Marine and Natural Resources together with BT, Dell, Eircom, the Irish Bankers Federation, IAB, Microsoft, Symantec, the National Centre for Technology in Education, Ward Solutions and Vodafone are working together to raise awareness of the urgent need for consumers and businesses to make their computers secure. This public–private consortium has created the second national computer security awareness campaign: ‘makeITsecure’. It is important to note that ISPs are part of the consortium.*
*Furthermore, the achievements of the awareness campaign have been monitored and communicated to the external world.*

# 7. Italy

Based upon the supplemented information from research and interviews, the following sections for Italy have been detailed:

# Local government as user of information systems

### Recent awareness programmes and initiatives

#### The Digital Youth Consortium

The Digital Youth Consortium is a non-profit organisation promoted by the city of Rome bringing together schools, training institutes, local public administration and ICT companies. The following companies have joined as founding members:

- Acea;
- Elea Engineering;
- eWorks;
- Wind Telecomunicazioni SpA;
- Unisys.

All these organisations have contributed to the constitution of the consortium fund.

The consortium addresses students, teachers, families and whoever is interested in improving relations between young people and computers, with obvious benefits in the field of didactics, work and productivity. Their activity is carried out mainly within the Rome area, where they carry out studies, research and activity plans.

The consortium promotes experimental projects which begin with computer literacy, to the development of programs and content which utilise the Internet and new technologies as pedagogical-educational tools. They also promote the Global Junior Challenge world competition.

*The objectives*

- To reinforce the use of new technologies in schools and didactic institutions, leading them towards the digital age;
- To promote the development of innovative educational environments which make use of new multimedia technologies;
- To facilitate the placing of young people in workplaces matching offer with demand;
- To identify the most qualified resources and strengthen the efficiency of workplace training.

#### The Global Junior Challenge

The Global Junior Challenge is a global award promoted by the Digital World Foundation ([26]), a non-profit organisation founded by the municipality of Rome and six major ICT companies. The intention of the award, dedicated to young people and to schools, is to identify and reward best practices on the use of new technologies in education and training of youngsters. An international jury selects the finalists. The winners are announced during the award ceremony that takes place in Rome, at the Campidoglio City Hall. The Global Junior Challenge is in line with the e-learning programme of the European Commission. The goal of this programme is to promote a digital culture between teachers and young people.

The Global Junior Challenge is dedicated to all young people, from school children to teenagers and youth taking their first steps on the job market. It concerns cities, institutions, local authorities, businesses, NGOs, communities and individual citizens. The Global Junior Challenge concerns all those who are interested or involved in child and youth education and training, and, more broadly, in helping in the construction of a more inclusive society.

The goal of the Global Junior Challenge is to develop exchanges of experiences between people in many countries. The spirit of the challenge is to facilitate the knowledge of different cultures and the use of new technologies among people all over the world. Thus, participants in the Global Junior Challenge, pursuing this philosophy, can be the protagonists of this process, building a network of partner projects and creating precious cooperation for further developments.

**The projects**

Several projects have been run by the Digital Youth Consortium. A brief description of the projects can be found below.

*Schools online*

This is the project aimed at schools, promoted by the city of Rome and managed by the consortium. It concerns Rome schools of all levels and types, and aims to stimulate the use of new multimedia technologies by students, particularly those who are less advantaged. The schools online initiative provides schools with a free web space allowing the creation and updating of websites, and also allowing development of multimedia projects and use of e-mail addresses. Students can also take advantage of computer training courses, in order to learn how to deal with problems connected to the use of the Internet. More details are available at http://scuoleonline.gioventudigitale.net

[26] Further details are available at http://www.gioventudigitale.net/en/index.asp and http://www.gjc.it/2006/en/index.php

*Training is considered the most effective technique. A comprehensive set of computer-based training and communication tools can help train end-users to ensure program effectiveness.*

*LEIPS — learning about e-learning processes in European schools*

Installing computers in schools is not enough to lead to effective e-learning processes. The e-learning action plan identifies 'management of change' as one of the key training themes to ensure the success of e-learning in Europe. This project aims to support and contribute to the success of e-learning within Europe through a systematic programme that combines the following activities:

- Knowledge generation on e-learning processes;
- Development of video and online multimedia training material;
- Testing of training material with stakeholders of European learning communities;
- Wide European dissemination of training material and knowledge sharing;
- Stimulation of a European network of stakeholders interested in the understanding, practice and transfer of e-learning innovation processes.

The project is coordinated by the Digital Youth Consortium and carried out in partnership with the municipality of Stockholm (Sweden), the municipality of Barcelona (Spain), the municipality of Naesteved (Denmark) and the Atenea/Censis Institute (Rome). More details are available at www.leipsproject.org

*Within this project, cooperation with other European countries has been actively pursued.*

*'Silver surfers' using the Internet ('Nonni su internet')*

From 26 October 2006, the 'silver surfers' of the city of Rome could attend information security awareness trainings. This initiative is one of many that have been organised by the Digital Youth Consortium to raise awareness for this target group.

In the course of 2007, other organisations[27] have run training courses for users over 65 in several Italian cities. These initiatives have been realised with the support of the private sector, local government and ISPs, such as Microsoft, Telecom Italia, Credito Valtellinese, the city of Rome and others[28].

*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 a broader audience within the target group. Several partners or multiplier bodies can be used to help deliver the messages as part of an initiative.*

*In Italy, some initiatives have been organised with the support of adult education programmes, banks, industry bodies (unions, associations) and ISPs. Specific channels, such as unions, security institutions etc. have been recognised as an effective way of communicating with 'silver surfers'.*

*Week dedicated to the promotion of digital knowledge* (Settimana dell'alfabetizzazione digitale)

The Digital Youth Consortium, with the help of 'silver surfers', young people and trainers who participated to the *Nonni su Internet* initiative, has invited citizens to go back to school and learn how to write a letter using a PC, how to use the online services provided by the public administration and how to send an e-mail. The initiative was held in Rome from 27 to 31 March 2006. The sponsor of the initiative is Engineering Ingegneria Informatica[29].

'Don't throw me away ... there is a place at the recreation centre for the elderly' *(Non mi buttare... Al Centro Anziani c'è Post@ per me!)*

The Digital Youth Consortium is collecting used computers from companies which have decided to get rid of them. Once collected, students of the city of Rome will reconfigure the computers focusing on enhancing security and usability. The first computers will be given to the 3000 'silver surfers' who attended the course 'Silver surfers using the Internet'.

## Government as a partner with business and industry

*A campaign addressing parents for the right use of new technologies by minors*

[27] This refers to universities for people over 65, cultural associations and unions, such as Mondodigitale, Interessi metropolitani, CGIL and others.
[28] Further details are available at http://www.repubblica.it/2007/06/sezioni/scienza_e_tecnologia/computer-over-65/computer-over-65/computer-over-65.html; http://www.lazioecitizen.it/web/guest/rassegna/2007/14032007over60
[29] Further details are available at http://www.eng.it/index_e.htm

The Ministry of Communications and the Department for Information and Publishing of the Prime Minister's office launched a campaign on the right use of new technologies by minors[30].

'To know technologies is the best way to help your child to use them properly', is the innovative logo of the campaign addressed to parents of youngsters aged between 9 and 14.

That means, while it becomes more and more urgent to foster new technologies and their potentials as a means of development and democracy all over the country, it is equally urgent that, on the basis of recent events, minors be protected from possible dangers coming from an uncontrolled use of technologies and, at the same time, making families aware of the above-said dangers and potentialities.

The campaign, which began on 14 June 2007, is organised into two phases, i.e. June–July and September. It will be broadcast on the main national radio and television networks, press and Internet portals.

The TV film, lasting 30 seconds, addresses itself in a friendly and ironic way to parents, aiming to spur them on to care about the computer world (it also illustrates mobiles and videogames). The film tells about a nice but a little awkward mother struggling with her son's computer. In the happy ending, mother and son are sitting in front of the computer, surfing the Internet and sharing information and discoveries.

The press and the Internet campaigns, meanwhile, use technical jargon which is well known to youngsters but new and unknown to parents.

This is a multi-subject campaign, contextualising technology terms inside phrases aiming to be misunderstood in order to make parents aware of their lack of knowledge of new technologies: 'strange URL coming from your son's room'; 'when your daughter wears bluetooth, everyone can see her'; 'your daughter does spamming but not in gym'; 'when there's a football match, your son goes streaming'.

This new initiative of the Ministry of Communications is part of a plan to safeguard minors. It began on 8 January 2007, following the approval of the decree which binds Internet providers to using filtering systems to prevent access to sites broadcasting pornographic and paedophilia images. This ministerial decree was followed by both the renewal of the agreement ruling the 114 children emergency services and the starting up of the Internet site

[30] Further details are available at http://www.comunicazioni.it/en/index.php?IdNews=185

www.tiseiconnesso.it[31]. The website advises youngsters, parents and teachers on the safe use of the network.

The campaign, planned by Saatchi and Saatchi, has been realised with the support of the Italian Providers Association (AIIP). The association ensured the presence of a banner in all affiliated sites. Besides, Vodafone Italia has planned to send a message to all subscribers of the MMS Mania service to make them aware of the responsible use of mobile phones[32].

*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 a broader audience within the target group. Several partners or multiplier bodies can be used to help deliver the messages as part of an initiative.*

*In Italy, some initiatives have been organised with the support of the Italian Providers Association (AIIP).*

*The message of the campaign is simple and tailored according to the target group interests', needs and knowledge level. Terms and definitions used should always be easy to understand by the intended target group.*

[31] Further details are available at http://www.tiseiconnesso.it/doc/comunicato_Sito_Minori.doc
[32] Further details are available at http://www.governo.it/GovernoInforma/Campagne/minori_nuove_tecnologie/index.html and http://www.tiseiconnesso.it/

# 8. Lithuania

Based upon the updates received on the contribution provided last year, the following sections for Lithuania have been detailed:

National government as user of information systems

Government as partner with business and industry

# National government as user of information systems

### Recent awareness programmes and initiatives

The project 'Strengthening capacities of authorities dealing with IT and data security' was implemented using PHARE funds in 2005.

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

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

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

*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.*

## Government as a partner with business and industry

**Internet service providers (ISPs)**

Meetings of national ISPs, market players and representatives of the Communications Regulatory Authority on NIS and the establishment of a national 'cert' took place between May and July 2005 and during 2006.

**Public–private partnership**

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

The new website dedicated to awareness of NIS went live in February 2006. The website is the result of the work of a public–private partnership[33]. The website www.esaugumas.lt is dedicated to Internet users, SMEs and State institution network administrators and is intended to be an interactive forum of NIS for all interested parties. Articles, news, a forum for discussions, advice on NIS issues, tools for users to avoid NIS incidents, etc. are all available.

In cooperation with banks, RRT prepared a brochure to inform users about phishing and ways in which to recognise those attacks and how to protect against them. Some 200 000 brochures were distributed throughout Lithuania.

RRT, in cooperation with well-known security vendors, has worked together on the project 'Safeguard your computer!' to produce a tool for home users, aiming at improving security on their personal computers. A CD-ROM with the collection of necessary safeguard programs (antivirus, antispam, antispyware and others) and relevant information about secure use of the Internet has been developed. About 100 000 CDs were distributed free of charge throughout Lithuania in June 2006. The final stage of the project was widely covered by the media.

[33] A full list of partners is available at http://www.esaugumas.lt/index.php?-952219156

Projects such as ‘Safer digital Lithuania’ (raising user awareness) and ‘Hotline Lithuania’ (directed against harmful information on the Internet) under the EU programme ‘Safer Internet’ are ongoing. Partners for the projects are JSC Bitė Lietuva, the Ministry of Education and Science, the Information Society Development Committee under the Government of the Republic of Lithuania, the Communications Regulatory Authority and other public and governmental institutions. The time frame of the projects is 2005–07.

*Public–private partnership can be a highly effective way to deliver campaigns especially if each organisation can leverage strengths and resources.*

# 9. Luxembourg

Based upon the updates received on the contribution provided last year, the following sections for Luxembourg have been detailed:

Local government as user of information systems

Government as partner with business and industry

# Local government as user of information systems

### Recent awareness programmes and initiatives

CASES has developed an awareness-raising campaign for local government. Upon the results of a risk assessment of a public entity, flyers, posters and an awareness-training presentation have been produced and have been deployed in one ministry. The campaign will be deployed on two more entities in 2007.



# Government as partner with business and industry

### Internet service providers (ISPs)

CASES has analysed the ADSL-routers sold by the Luxembourg ISPs. Strength and weaknesses of the routers have been published ([34]). Upon this publication, the main ISP (P & T) has changed one router because it was not secure enough.

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

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

Another project which involves ISPs and mobile phone providers will go live at the beginning of September 2007. The project aims at fighting cyber-bullying.

[34] More details are available at http://www.cases.public.lu/publications/dossiers/dsl/index.html

# 10. Malta

Since the publication of the Information Package 2006, no further government initiatives have been undertaken by ISPs to raise information security awareness among users. Thus, the following section for Malta is still valid:

Government as partner with business and industry

## Government as partner with business and industry

### Internet service providers (ISPs)

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

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

# 11. Netherlands

Since the publication of the Information Package 2006, no further government initiatives have been undertaken by local government and ISPs to raise information security awareness among users. Thus, the following sections for Netherlands are still valid:

National government as user of information systems
Local government as user of information systems
Government as partner with business and industry
Government as partner with civil society

## National government as user of information systems

### Recent awareness programmes and initiatives

*ICTU*[35]

The ICTU foundation was established on 11 April 2001 by the Ministry of Home and Kingdom Affairs. The motto of ICTU is 'Helping government achieve better results with information and computer technology (ICT)'. ICTU combines knowledge and experience in the field of ICT and government. ICTU carries out various programmes for and in cooperation with governmental organisations. Policy is translated into specific projects for government. In the board of ICTU all layers of government participate: State government, provinces, local communities and district water boards.

## Local government as user of information systems

### Recent awareness programmes and initiatives

*EGEM*[36]

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

EGEM has an eye for things already developed by councils and has undertaken the task of spreading the existing knowledge: 'Crib, imitate, EGEMulate'. Local councils which would like support for specific issues at implementing e-government projects can use EGEM-i[37].

## Government as partner with business and industry

### Internet service providers (ISPs)

There does not seem to be any cooperation between ISPs and the government with the exception of the Dutch hotline. The branch of industry NLIP no longer exists and without support from the government, the hotline for illegal content is not operational.

[35] Text quoted from: http://www.ictu.nl/profile.html
[36] Text quoted from: http://www.ictu.nl/profile.html
[37] The 'i' stands for implementation or introduction.

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

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

## Government as partner with civil society

### Public–private partnership

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

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

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

- Education of children, teachers and parents on the potential risks of the Internet — this follows several incidents involving youngsters and either paedophiles, online bullying or unwanted online experiences. Several initiatives have been launched to reach children, teachers and parents, among which are a code of conduct for chat rooms (coordinated by ECP.NL), sites for parents and teachers (by the major Dutch Internet provider KPN Internet) and the activities of the current Dutch awareness node NaNSoS. These include sending information materials to all Dutch schools, being present at the main Dutch educational fair, and organising the Safer Internet Day 2006 (with the theme ‘Let children teach the grown-ups about Internet safety!’). Moreover, NaNSoS is active in promoting the Dutch Internet certificate (developed

under the label of the awareness node by the Ministry of Economic Affairs, for primary schools and officially launched in October 2005. The approach taken is not one of 'ban and control', but rather one of 'educate and instil responsibility';

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

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

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

*Results*

The first tangible result of the national Digibewust campaign was the joint celebration of Safer Internet Day 2006, where the national awareness node organised a number of activities together with private organisations such as Microsoft, UPC, KPN, ANWB, TPG and IBM. Several public bodies and NGOs also organised activities including the Dutch consumer

organisation, Govcert, and the ICTU. A massive multimedia campaign was launched which will actively take part in promoting and organising activities.

*The role of the proposed awareness node*

The proposed awareness node will continue the work performed under the current NaNSoS awareness campaign. The node will closely cooperate with all relevant national parties and especially with the Dutch government, the intended co-sponsor of the awareness node. Moreover, cooperation with other European countries will be actively pursued.

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

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

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

*Public–private partnerships can be a highly effective way of delivering campaigns, especially if each organisation can leverage strengths and resources.*

*In the Netherlands, the Netherlands Ministry of Economic Affairs has decided to intensify the existing awareness campaign SurfopSafe and align it with other activities, both from the government itself as well as those from private parties. A massive multimedia campaign was launched to promote and organise activities.*

# 12. Norway

Based upon the updates received on the contribution provided last year, the following sections for Norway have been detailed:

Government as partner with business and industry

Local government as user of information systems

## Government as partner with business and industry

**Internet service providers (ISPs)**

The website www.nettvett.no was launched on 26 April 2005 and is a collaborative project between several government entities and ICT businesses, including several ISPs.

The website provides information, advice and guidance for the secure and safe use of information and communication technology when using the Internet and its applications. As it is an awareness-raising initiative, the aim is to contribute to the increase of knowledge among the general population and SMBs within the field of information security. The themes that are covered are, among others:

- Secure connection to the Internet;
- Back-up;
- Secure and safe use of e-mail;
- Spam;
- Phishing;
- Protection against loss of data;
- Confidentiality issues;
- Protection against attacks from the Internet;
- Securing your wireless network;
- Use of digital signatures;
- Security regarding use of mobiles.

The information on this website is presented in a logical way dividing the themes into several categories. The information is also categorised into knowledge levels such as ‘for beginners’, ‘more advanced users’ and ‘for businesses’. For most of the theme categories, the website also gives short and easy to remember rules for what to be aware of when using the different Internet applications. The users can also post questions to the website if they have questions related to the content on the website or related themes.

Through a marketing campaign, Nettvett.no will try to get more people to take backups of personal information and data. By developing an animated guide, nettvett.no aims to make private consumers see the importance of taking backup of their personal data. The campaign is a result of the cooperation between nettvett.no and electrical retailers. National Security Day is 24 April and a seminar will be held. The focus was on small and medium-sized enterprises. They have also worked together with NorSIS and SAFT with the development of a TV programme for children. The programme will try to explain Internet security issues in a simple way.

The plan is to have Nettvett.no as the leading national governmental website providing the public and SMB with the most up-to-date information, advice and guidance within the field of information security. This will include secure and safe use of the Internet and Internet applications.

## Local government as user of information systems

### Recent awareness programmes and initiatives

In 2005, the municipality of Baerum produced a film on the importance of information security. The film, named *Baerum safe — a film on information security in Baerum municipality*, is part of a local awareness-raising programme aiming at increasing the level of information security knowledge among the 3 000 employees of the municipality of Baerum. The film is roughly 10 minutes long. The main purpose of the film is to demystify the concept of information security and point out the similarity to other types of security. Moreover, with this initiative the municipality tried to:

- Raise end-users' information security awareness: informing end-users on their own responsibility of Baerum's information security and on their ideal general information security behaviour, for instance:
    - End-users are responsible for the protection of their passwords,
    - Log off their PCs at the end of the day,
    - Pay attention to social engineering attempts,
    - Understand the division of security responsibilities between the IT department and the end-users[38];
- Reduce the overall cost of trainings — prior to the film, the IT officer was organising and running information security induction trainings for the new comers of the municipality. After having analysed the impact of this activity on the operations of the IT office and the related costs, the municipality decided to have line managers be in charge of information security training as part of general induction courses and to produce the *Baerum safe* film to be projected during the training sessions. This new approach led to some cost savings and, was effective in disseminating the message to new employees.

In 2005, the IT officer at Baerum municipality and author of the film, was awarded with the good information security work prize by KInS, the Association of Municipal Information Security in Norway. Since then, the film has been modified and adapted by KInS and the Norwegian Centre for Information Security (NorSIS). At present, KInS and NorSIS, in

[38] The IT department of the municipality is responsible for the technical aspects of security like installation and maintenance of firewalls and anti-virus application.

cooperation with the Norwegian Data Inspectorate, shows the film at management seminars all around Norway. In addition, several copies of the film have been sold to other Norwegian municipalities which, just like Baerum, use it to raise awareness among their employees.

More information on NorSIS can be found at: http://www.norsis.no

*It is important to evaluate the return on investment (ROI) of any information security awareness programme.*

*In Norway, the analysis of costs in trainings led the municipality of Baerum to decide to use a different channel to increase the information security knowledge of their employees. A film was produced*.

# 13. Portugal

Since the publication of the Information Package 2006, no further government initiatives have been undertaken by local government and ISPs to raise information security awareness among users. Thus, the following sections for Portugal are still valid:

Local government as user of information systems
Government as partner with business and industry

## Local government as user of information systems

**Recent awareness programmes and initiatives**

Local governments, due to the nature of the political organisation of the country, have no activities in this area.

## Government as partner with business and industry

**Internet service providers (ISPs)**

Cooperation between the government and ISPs has not been directly organised by the government but through Fundação para a Computação Cientifica Nacional (FCCN)[39], the organisation running the Portuguese NREN.

In Portugal, there are a number of ISPs and in recent years there has been a significant increase in the use of broadband technologies (cable and ADSL). There are also an increasing number of hotspots where broadband access is available. Due to the nature of these technologies, ISPs have been active in distributing information to their customers of the specific problems of these technologies due to the increasing potential of problems as a result of always-on networks and higher available bandwidth.

For around two years, FCCN has organised periodic meetings with ISPs to discuss measures to be taken by this economic sector to control security problems. For ISPs, the most relevant problem is spam and the problems related to malicious mail. A forum has been created where ISPs share information about security problems and the techniques and solutions each of them is taking to solve these problems. Although they are competing in the market, this is an area where it is agreed that cooperation is beneficial.

A project is just starting to develop a platform for information sharing concerning black lists of spammers to be interchanged among ISPs. FCCN will be the coordinator of this project. Together with this initiative each ISP is launching (addressed to its customer base), some initiatives dedicated to awareness-raising in the security area, namely with details of good practices in the area.

[39] Further details are available at http://www.fccn.pt/

# 14. Spain

Based upon the Information supplemented from research and interviews, the following section for Spain has been detailed:

Local government as user of information systems

# Local government as user of information systems

### Recent awareness programmes and initiatives

### CESGA information security campaign

The Supercomputing Centre of Galicia (CESGA) is the centre for high-performance computing, communications and advanced services used by the scientific community of Galicia, the university academic system and the Consejo Superior de Investigaciones Científicas.

CESGA works through two institutions:

- Fundación Centro Tecnolóxico de Supercomputación de Galicia (CESGA Foundation);
- Sociedade Anónima de Xestión Centro de Supercomputación de Galicia (SAX CESGA).

The CESGA Foundation aims to promote and render high-performance computing and communications services to the research communities of Galicia and CSIC, as well as to those companies or organisms which request them. The foundation aims at improving competitiveness among companies by means of technological development and innovation.

Its primary functions are:

- To supply high-performance computing and advanced communication services to the users;
- To administrate the science and technology network of Galicia;
- To promote and develop cooperation among companies and institutions.

SAX CESGA meanwhile aims to promote support services for research, development and innovation in the field of IT and communications in Galicia and in the scientific community of CSIC.

Its primary functions are:

- To promote the use of high performance computing technologies and advanced communications;
- To promote the use of technologies related to the knowledge society, including e-business, e-learning and geographical information systems.

In the fourth quarter of 2006, as part of its activities, the centre launched an information security awareness initiative targeting SMEs. Galicia is characterised by a lack of confidence and knowledge in some areas of ICT. Thus, there is a massive rejection of the use of Internet services, mainly related to e-commerce. Given the importance of entrepreneurial initiatives in Galicia, the objective of this project is to help SMEs understand the risks and threats that could have an impact on their business while using the network[40]. Different activities have been organised including seminars, courses and dissemination events. Different channels have been used to deliver the message of this initiative:

- Website;
- Brochure/magazine;
- Seminar/meeting/conference;
- e-newsletter/email;
- Training.

The awareness initiative is scheduled to end in 2008 with the possibility of an extension.

*It is important to use multiple channels to deliver the awareness-raising messages. In Spain, offline and online channels have been used.*

[40] Further details are available as follows:
e-commerce guide (in Galician): http://www.e-negociogalicia.com/formacion/comercio-e/seguridade.html;
articles in the centre's magazine: http://www.e-negociogalicia.com/revista/anteriores;
security as part of some reports (in Spanish, Galician, and English): http://ichnos.e-negociogalicia.com/component/option,com_docman/task,cat_view/gid,15/Itemid,27/lang,en/;
interoperability: http://ichnos.e-negociogalicia.com/component/option,com_docman/task,doc_details/gid,38/Itemid,27/lang,en/;
security as part of massive regional surveys: http://www.e-negociogalicia.com/observatorio/informes/;
security in other reports: http://www.e-negociogalicia.com/xestion_web/contenidos/Regional_ICT_and_e-Commerce_Report.pdf; http://www.e-negociogalicia.com/observatorio/informes/outros

# 15. Sweden

Based upon the updates received on the contribution provided last year and on the supplemented information from research and interviews, the following sections for Sweden have been detailed:

Local government as user of information systems
Government as partner with business and industry

# Local government as user of information systems

### Recent awareness programmes and initiatives

Sweden has around 290 local governments altogether. Given this number, it has been possible to gather data on a few information security initiatives that have been undertaken or are in progress in Sweden.

*The Swedish Association of Local Authorities and Regions*

The Swedish Association of Local Authorities and the Federation of Swedish County Councils represent the governmental, professional and employer-related interests of 290 local authorities, 18 county councils and two regions. For more information, refer to http://kikaren.skl.se/artikel.asp?C=756&A=180

The association and the federation strive to promote and strengthen local self-government and to create the best possible conditions for the work of their members. Membership fees largely finance the activities.

The association has published information on information security policy adapted to local and regional authorities. Security issues are discussed at conferences and best practice from a local authority could be highlighted. Information such as advice on new and relevant legislation is published on the website.

*City of Stockholm film initiative*

Citizens must be confident about how their personal information is handled and how services are offered. They rely on the fact that the city of Stockholm employees are well trained and aware of the importance of security when delivering the services.

The city of Stockholm has produced a film based on the new policy and guidelines for information security (decided during autumn 2005). This is an attempt to make end-users aware of what information security is about from their own perspective. The film contains a number of interviews with employees and some partners to the city of Stockholm. Every interview is based on a chapter from the new policy and guidelines. The chapters of the guidelines, as illustrated in the film, cover areas such as administration, responsibility and methods as well as technical subject areas.

One topic refers to the social welfare system which is one of the most important systems for the city of Stockholm. Some employees, such as a system owner, a system administrator and a local handling officer describe their role-specific responsibilities.

Physical security or perimeter security is another issue described in the film; aspects of mobility such as working with hand-held computers and the risk of using wireless connections are covered.

A risk analysis exercise from a local borough in the city is also presented. The chapter emphasises the importance of e-security and the necessity of having top management supporting the work.

In 2005, the city of Stockholm also published a leaflet aimed at raising information security awareness. The decision to produce a leaflet followed a city council decision of 2005 when revised versions of the city's information security policy and guidelines were formally put into place. The objective of the leaflet was to raise awareness of the existence and overall content of this information security policy and guidelines.

The security leaflet addresses employees in the city of Stockholm in general with particular focus on the management level. The target group not only comprises line managers within the administration and municipality owned companies, but also politicians.

Under a number of headlines, the leaflet covers what was regarded as the most important for everyone to understand with regard to organisation and administration of information and IT systems, including the following:

- All staff must know who is in charge of the city's information security;
- All staff must possess basic security knowledge;
- All information must be kept securely;
- Access to IT systems shall be granted formally and only based on need;
- The basic security level shall be determined by an information classification.

As the leaflet only consists of 11 pages and since half of them display images for illustrative purposes, the strategy has been to use the leaflet as a 'door-opener' to the city's intranet. From the city intranet, the policy and guideline documents, advice and instructions, and information security manuals can be downloaded.

Over 1 000 copies of the leaflet have so far been printed and distributed within the city administration. The leaflet has been very well received and some parts of the administration even ordered supplementary copies of the leaflet.

*Municipality of Örnsköldsvik*

In April 2007, the municipality of Örnsköldsvik implemented an information security education programme as part of its overall information security strategy. The programme is based on the e-learning system DISA[41] developed by the Swedish Emergency Management Agency.

The training targets all employees of Örnsköldsvik municipality aiming at increasing their level of information security awareness as it has been recognised that the level of knowledge of this target group is quite low. The objective is therefore to offer the training as part of any other important staff training.

The training comprises three modules: 'Introduction', 'Basic information security' and 'Manager's responsibility'. The first two modules are mandatory for all employees, while only line managers are required to complete the last one, manager's responsibility.

Each module introduces a set of organisational security rules explained under topics like 'Your workplace', 'Your authorisation', 'Internet' and 'Email'. In addition, a number of practical cases are included. Each one of them illustrates the risks associated with the different security topics.


The e-learning system DISA can be integrated with an advanced tool enabling the organisation to monitor the number of users who have completed the training, analyse their results or progress, and act upon them. This information can be used to demonstrate differences in knowledge, needs and interests within the organisation. This tool has proved to be an efficient way of preventing the training's implementation pace to decelerate too much.

[41] DISA stands for *Datorstödd InformationsSäkerhetsutbildning för Användare* (computer-based information security education for end-users). DISA solutions were designed to fit any municipalities and governmental agencies to deliver customer solutions.

More information on DISA can be found on the Swedish Emergency Management Agency's website (in Swedish) at http://www.krisberedskapsmyndigheten.se/disa

*Specific channels have been used during this initiative. The training comprises of three modules: 'Introduction', 'Basic information security' and 'Manager's responsibility'. The first two modules are mandatory for all employees, while only line managers are required to complete the last one, manager's responsibility. The messages delivered have been tailored for the target group interests', needs and knowledge level. Moreover, this experience has been made more interactive*.

## Government as partner with business and industry

### Internet service providers (ISPs)

No information is available in a suitable format at this time. Many operators provide security information on their websites.

# 16. United Kingdom

Based upon supplemented information from research and interviews, the following section for the United Kingdom has been detailed:

Local government as user of information systems

# Local government as user of information systems

### Recent awareness programmes and initiatives

The Manchester Digital Development Agency (MDDA) is a public sector organisation funded by the European Regional Development Fund, the Manchester City Council and the Northwest Development Agency. MDDA offers impartial advice and services about ICT to organisations, home users and small and medium enterprises in greater Manchester.

Delivering its services at a local and regional level, MDDA supports a range of initiatives that, among other things, include collaborating with local authorities across greater Manchester to share good practice and work together on joint projects. MDDA also works with communities to use new technologies to ensure better access to local services and they provide business support to enable small businesses to benefit from broadband technologies through working with different partners.

As part of the Broadband for Communities project, the MDDA technology team offers a number of workshops and services, such as the so-called 'Basic security'. Targeting home users and SMEs, the goal of this programme is to raise security awareness and to improve IT skills. MDDA estimates the level of information security knowledge of these target groups as low.

This training helps to inform about the risks from the unwanted effects of viruses (such as trojans and worms) and spyware, the responsibilities of data protection and how to protect PCs and stored personal details from such threats. The workshop outlines the practical and technology implications for IT systems with examples of software to help tackle these problems. The activity was designed in response to requests from local groups. The technology team uses a number of laptops and discussion to demonstrate the features and issues relating to keeping PCs secure. The duration of the workshop is approximately two and a half hours.

Some of the themes covered include:

- Basic computer security terminologies;
- The security implications such as when sharing files and connecting to the Internet;
- Prevention using common security software such as antivirus, firewall and anti-spy ware;
- Security features included in Windows;
- Contingency measures such as backing up;
- Practical measures such as physical security.

A number of different channels were used as part of delivering the message of the awareness programme. Apart from a website and training, fact sheets and e-newsletters have been used. The basic security workshop has been available, free of charge, from the last quarter of 2006 until June 2007.

The website of the Manchester Digital Development Agency is: http://www.manchesterdda.com/

Information on the Broadband for Communities project can be found at: http://www.manchesterdda.com/article/100/

# Other organisations' good practices

## *Vodafone*

Vodafone is the world's leading international mobile telecommunications group with 198.6 million customers, calculated on a proportional basis as at 31 December 2006, with approximately 30 million of these customers using their devices to access Vodafone live! and the mobile Internet[42].

One of Vodafone's 10 business principles commits the organisation to providing customers with safe reliable products. On this basis, a steering group was set up in 2003 to protect their customers from inappropriate content, contact and commercialism by ensuring that services and products are delivered responsibly for:

| | |
|---|---|
| Commercial content | Broadband and DSL propositions |
| Social networking products and services | Parental controls mechanisms |
| Marketing of age-sensitive content | Mobile advertising |
| Spam and P2P malicious communications | Location enabled services |

Between other actions, in 2005 Vodafone made an external commitment to implement parental controls solutions that would prevent inappropriate access to age-restricted content and services by March 2007.

The firm's access controls prevent children accessing 18-rated content on the Vodafone live! portal by either requiring users to verify their age as 18 or over, or by enabling parents to select a profile for their child that will remove 18-rated content.

Their Internet filter enables parents to prevent their children accessing inappropriate age-restricted content on Vodafone live! via their mobile phones. The access control has been introduced in four operating companies in the 2007 financial year, making it available in a total of six markets (i.e. Germany, Italy, the Netherlands, Portugal, Spain and the UK). For example, in the UK, a default content control bar is applied to all consumer customers. The

[42] Further details are available at http://online.vodafone.co.uk/dispatch/Portal/appmanager/vodafone/wrp?_nfpb=true&_pageLabel=template10&pageID=PAV_0014

bar can be removed if customers are able to verify that they are 18 years old or over. Age verification can be done by credit card registration or proof of age.


The solution continues to be rolled out with new operating companies, such as in the Czech Republic, setting targets to implement a filter by March 2008. Local operating companies that have not yet implemented the filter will create a 'walled garden' by removing access to the Internet completely on request by customers.

Some local operating companies also provide Internet filters for content on the worldwide web, outside Vodafone live!. This system enables parents to prevent their children accessing inappropriate age-restricted content on the Internet via their mobile phones. It is now available at two local operating companies (i.e. Japan and the UK) and nine additional operating companies have set target dates for implementation. Vodafone planned to offer Internet filtering solutions in all markets by March 2007.

Vodafone continues to review the requirements and it has been noticed that education and awareness campaigns are important to ensure that parents are empowered with the requisite information to make the best decisions concerning their children and the Internet.

Furthermore, bulk unsolicited communications, or spam, are a source of irritation for mobile users. Vodafone never sends spam but third parties use their networks to send marketing messages to Vodafone customers. Messages inviting customers to call or subscribe to premium rate services can be particularly problematic. Vodafone is tackling spam at both ends: monitoring unusually high sending patterns and disconnecting the sender, as well as providing spam filters for their customers to screen out unsolicited messages.

The full report on content standards is available at:

http://www.vodafone.com/start/responsibility/consumer_issues/content_standards.html

## *France Telecom*

In July 2000, France Telecom was one of the first French companies to join the Global Compact[43]. This public commitment is the expression of willingness to pursue growth in a responsible manner. It also allows the organisation to declare and promote some principles that are shared by all employees via the company's code of ethics. France Telecom's support for the Global Compact's 10 principles forms a universal framework of reference, to the advantage of their customers and, more generally, all of its stakeholders.

France Telecom has been involved in some initiatives to implement their strategy for 'responsible growth'. They are also the expression of the company's overall motivation and that of all its employees.

As part of the initiatives to promote the correct use of services, the flexible parental control tools developed by Wanadoo is one of them. The tolls are available from the home page of its Internet site (www.wanadoo.com). In association with Bayard and the Forum des droits sur l'Internet (Internet Rights Forum), Wanadoo also offers access to around 100 chat sites, catalogued according to age (under 18, 18-25, etc.) with elementary educational information, such as: do not arrange to meet someone you don't know, do not give out sensitive personal information, etc. Wanadoo has also organised various types of active protective action for customers in order to sanction or help sanction the authors of anything offensive.

As another example, customers with children just need to call customer service and Orange can restrict access to the content of certain sites or implement a system of moderation for the use of chat sites, blogs and instant messaging. This is mainly aimed at preventing illicit activity and protecting users from malicious outsiders.

Information campaigns about correct usage are also organised with the aim of improving quality of life.

Orange has implemented a campaign to raise awareness of the nuisance that can be caused by mobile telephone ringtones in public places, public transport, etc.

---

[43] In an address to the World Economic Forum on 31 January 1999, the former Secretary-General of the United Nations, Kofi Annan, challenged business leaders to join an international initiative — the Global Compact — that would bring companies together with UN agencies, labour and civil society to support universal environmental and social principles. The Global Compact's operational phase was launched at UN Headquarters in New York on 26 July 2000. Today, thousands of companies from all regions of the world, international labour and civil society organisations are engaged in the Global Compact, working to advance 10 universal principles in the areas of human rights, labour, the environment and anti-corruption. Through the power of collective action, the Global Compact seeks to promote responsible corporate citizenship so that business can be part of the solution to the challenges of globalisation. In this way, the private sector — in partnership with other social actors — can help realise the Secretary-General's vision: a more sustainable and inclusive global economy. Further details are available at http://www.unglobalcompact.org/AboutTheGC/index.html

In France, in partnership with regional authorities, the company has implemented solutions allowing real-time broadcasting of information to citizens via channels chosen by the authorities. Warning messages can be sent (floods, pollution, major risks) as well as messages between municipal authorities and those that they administer (schools, day-nurseries, official services, etc)[44].

[44]France Telecom, participant in the Global Compact, FT / DRE & DD, 19 September 2005, p. 17. The document is available at http://www.search.francetelecom.com/en/?mot=parental+control&ok.x=7&ok.y=7

## *T-Mobile*

T-Mobile International is one of the world's leading companies in mobile communications. As one of Deutsche Telekom's three strategic business units, T-Mobile concentrates on the most dynamic markets in Europe and the United States. By the end of 2006, more than 106 million customers were served in the 12 T-Mobile markets. T-Mobile is a partner of FreeMove, an alliance formed by four of Europe's leading mobile companies — Orange, TIM (Telecom Italia Mobile), TeliaSonera and T-Mobile — to help their customers communicate as easily while travelling abroad as they do at home.

T-Mobile International, a wholly-owned subsidiary of Deutsche Telekom, was established in December 1999. Since then, it has positioned itself as one of the largest international mobile communications carriers[45].

T-Mobile is also offering a service to restrict adult content: Web Guard. Web Gard is a security feature that allows the primary account holder (PAH) to implement restrictions to adult-orientated content. Web Guard can be added to the following account types: Post Paid, Take ControlSM, and SmartAccess accounts. Web Guard is a required feature for kidConnectSM accounts.

While the Web Guard feature is designed to prevent access to certain types of restricted content, it is not foolproof. Account holders should still monitor access to content by mobile users on their account.

- Web Guard is an optional, add-on feature for post-paid customers;
- Web Guard restricts access to adult-themed (over-18) content on your phone;
- Customers designated as the PAH can add or remove Web Guard via My T-Mobile, the Sales Office or by contacting Customer Care;
- Web Guard can be turned on using the mobile phone, but cannot be turned off from the mobile phone;
- Web Guard is available on specific rate plans only;
- Customers on family plans may apply Web Guard to individual phones or all phones on their account;
- There is no charge to enable or disable this feature; it is free of charge;
- The feature targets Web access data plans and covers browse and search;
- Web Guard does not block or filter user-generated content, such as messaging, of any type;
- As with all technologies, the Web Guard filtering technology is not 100 % foolproof and so the filter may not work on a particular site or at some particular time[46].

[45] Further details are available at http://www.t-mobile-international.com/CDA/about_t-mobile,2,0,,en.html

Furthermore, to prevent identity theft, T-Mobile employs strict security measures, including password validation and account verification, to protect our customers' personal information. In addition, T-Mobile provides ongoing training to our customer service representatives and administers call-quality programmes. All of this ensures that, as best as possible, we only deal with authorised users. T-Mobile also complies with all applicable federal and state regulations regarding the care, use and disclosure of customer information[47].

[46] See http://support.t-mobile.com/knowbase/root/public/tm23351.htm#top
[47] See http://support.t-mobile.com/knowbase/root/public/tm23340.htm#top

## *Orange UK*

Orange UK is a mobile network operator and internet service provider in the United Kingdom which is owned by Orange SA, a subsidiary of France Télécom[48].

Education plays a key role within the Orange community. As a result, Orange UK is involved in a number of educational initiatives[49]. They include:

*Incoming message*

Incoming message is a free 10 minute film on DVD plus web based resources about bullying by text, for teachers of PSHE/PSD (Personal, Social and Health Education / Personal and Social Development).

Aimed at 11 – 14 year old students, it uses a fictional story line based on the experiences of young people who have been text bullied via their mobile phone. The film is supported by a range of downloadable activities developed to generate discussion and debate among students.

*You, your phone and staying safe*

This is a free resource for teachers of English, PSE/PSD and Citizenship. Using Orange's safety campaign as a case study, the aim of this resource is to raise awareness and educate 14-16 year olds about how to stay safe with their mobile phones. A key factor of 'you, your phone and staying safe' is that the materials students will be working with are real life examples from the campaign.

*Orange safety*

Orange provides information and advice to help users and their family use Orange's services safely.


Details on offensive content, bullying, harassment, socialising online, spam, online security and many other topics are available on the Orange UK web site. This information is provided for both mobile[50] and broadband[51].

[48] Further details are available at http://www1.orange.co.uk/about/index.html
[49] Further details are available at http://www1.orange.co.uk/about/community/education.html
[50] Further details are available at http://www1.orange.co.uk/safety/mobile/152/155.html
[51] Further details are available at http://www1.orange.co.uk/safety/broadband/index.html

In particular, Orange offers a service called ‘Safeguard’. It’s a filtering system for managing internet content. It works by preventing anyone under 18 years old from accessing adult content, while leaving them free to surf the rest of the internet. All Pay as you go accounts have Orange safeguard. Pay monthly customers don’t, as they’ve been through a credit reference check so should be over 18 years old.

Finally, in the section talking points advice to parents is given to help them discussing the issues of information security with their children, as well as pointing them in the right direction for finding out further information both online and locally about this matter[52].

[52] Further details are available at http://www1.orange.co.uk/safety/talkingpoints/

## *VigiTrust*

VigiTrust do not partner with the Irish government as such in terms of awareness programmes and initiatives. However, VigiTrust is engaging with a number of public sector bodies (government departments, local government and semi-rate organisations) to provide security awareness training. This is aimed at raising the overall level of security knowledge for all those attending the training. Attendees may choose to attend public workshops where they are taught together with private organisations or choose workshops that can be customised to the requirements of a particular government organisation and be held at their offices.

Since 2006, VigiTrust has almost completely moved away from half-day workshops and is now delivering 80 % of its workshops as one-day workshops, 15 % as two or three day workshops and the rest as half-day workshops. It has been recognised by participants that a one-day workshop is really more effective as more information is covered (e.g. the attendee should complete a draft plan of action on which the end-users and VigiTrust can follow up very proactively).

The organisations had good success in running awareness workshops on specific topics as opposed to generic introduction workshops such as:

- Workshops on ISO 27001;
- Workshops on PCI DSS Standard;
- Workshop on La loi sur la securité financière (France only);
- Workshops on disaster recovery and business continuity.

As last year, workshops on secure printing are still running.

In addition, since 2004 there has been an increase in the number of customers engaging in security programmes including awareness raising and deployment of policies. The main driver seems to be compliance with data protection or industry requirements to adhere to a specific standard such as ISO 27001 or PCI standard requirements.

*Target audience description*

IT technicians, IT directors as well as directors or chief executives for government departments attend the training with a view to getting more information about the legal, commercial, operational as well as technical aspects of corporate security. In order to raise awareness, VigiTrust looks at the business side of security rather than purely concentrating on technical security. Five security pillars are covered: physical security, people security, data security, IT security and disaster recovery/business continuity.

*Level of knowledge*

This varies and goes from low to high, but most attendees' knowledge before attending the workshop is between medium and low.

*Main issues*

The attendees seem to be focused on operational issues such as DR and BC and resolving issues linked to AV outbreaks. Very few are even aware of their responsibilities under the Data Protection Act and other key legislation.

Where customised workshops are being delivered, most attendees have different understandings of the security requirements and countermeasures at their government office. Most of them tend not to have clear policies and those policies that do exist are not communicated or enforced effectively. To that effect, it would seem that, in Ireland, the public sector has the same issues and overall level of knowledge in terms of legal requirements as regards to security.

At a technical level, government organisations on average are more advanced than their private firm counterparts for similar-sized organisations. They will tend to have content filtering for mail and web in place, as well as continually be looking at emerging threats such as USB memory stick usage and desktop threat management.

*Value added for attendees — how workshops are increasing security awareness levels*

Typically attendees leave with a SWOT (strengths, weaknesses, opportunities, threats) analysis on their environment looking at how security can be considered a strength, weakness, opportunity or threat for the organisation. Therefore they leave with a basic benchmark of their knowledge of the security status at their office against best practice. Then they are told how to prioritise action items and how to sort items from what can be done internally by existing staff and what should really be done by external security experts.

The feedback from Irish government customers is that they use the knowledge gained at the workshop as a platform to formulate a plan to further disseminate the concept of security awareness within their department. Very often the organisation formulates a plan on how to improve security levels based on the findings of the workshops.

*Metrics and KPIs*

Metrics are not officially in place. The effectiveness of the campaign can be measured by the attention it gets both from the media and the general public and by the hits on their website.

The idea of conducting a SWOT analysis of an organisation's security is a good start for establishing a base for that organisation's security awareness across the five key security pillars. By comparing the results of the first SWOT analysis with the results of a second analysis carried out after an agreed time frame (e.g. every six months), it is possible to establish the effectiveness of the awareness programme by looking at the following items.

- Have all the key threats been addressed?
- Have all the key opportunities to use security as a business enabler, as a company culture enhancement platform and as a productivity enhancement tool been utilised?
- Are the strengths identified in the first SWOT still there and are there more strengths after the second one?
- Have all the weaknesses been eradicated or mitigated?
- Are all employees aware of the changes?
- Are all employees more security aware?

The following items could be considered as a sample of a SWOT analysis results:

| | |
|---|---|
| **Strengths**<br>• Best-of-breed technical solutions are already in place.<br>• IT staff are aware of the main issues.<br>• Some policies are already in place.<br>• Qualified technical staff hold security accreditation.<br>• Management are supporting the IT team by way of financial commitment. | **Weaknesses**<br>• No general awareness of or commitment to addressing corporate security risks.<br>• Organisation X not maximising on previous investment on IT system and existing security features. Similar for procedures and policies.<br>• Day-to-day focus on security issues as opposed to long term strategy to eradicate issues or address them proactively.<br>• No accountability — no official security officer (SO).<br>• No policy consistency between the various arms of the group.<br>• Some policies missing, others need to be updated or rewritten. |
| **Opportunities**<br>• Additional IT resources are now in place, freeing up time for existing staff to focus more on security topics.<br>• There is an opportunity to use security to boost productivity, increase system availability and | **Threats**<br>• Lack of understanding, commitment and focus from management as regards overall corporate security risks.<br>• Hackers — no pen testing ever conducted on Rehab's systems. |

| | |
|---|---|
| reduce potential liability. This project will also enhance team spirit.<br>• Legal aspects of corporate security can be used to get commitment from senior management.<br>• A new CEO is being appointed — new working practices might be implemented to increase security whose priority level might go up on the agenda. | • DR? — No plan in place.<br>• Human behaviour — users not trained at all.<br>• Reliance on third-party security for the Intranet and websites, more reliance moving forward when moving to data centre. |

Other ways to measure the effectiveness is to look at the number of security incidents before the awareness programme started and after. For instance, how many virus outbreaks have been reported, how many cases of Internet abuse (browsing non-work related and/or offensive websites) have been detected, how many employees have received basic awareness training thanks to the programme and are these employees more productive than other employees who did not receive the training[53].

[53] More information on how measuring the effectiveness of awareness programmes and in particular on why counting security incidents, see *Information security awareness initiatives: current practice and the measurement of success*, ENISA, July 2007, pp. 14–20.

# Good practice guidelines

Based on the analysis of the information security initiatives described above, this report provides good practice guidelines that can be customised by the Member States to help facilitate their work on awareness raising.

The good practice guidelines comprise:

- Recommendations — general recommendations have been listed below and a full description is provided. When sample of good practice guidelines are identified within case studies reported, the name(s) of the Member State(s) implementing such recommendations is mentioned. This list should not be seen as comprehensive source of all good practice initiatives which have been undertaken and are reported in this document. This serves as help to readers to customise and implement these guidelines in their country. Recommendations also point out obstacles to success and provide practical advice on how to overcome them during the different phases of programmes;
- Checklists — breaking down each phase of an awareness campaign into tasks and activities, checklist items can be constructed. Member States could use these as guidance for the main steps to undertake when running information security awareness-raising programmes;
- Roadmap — the diagram should only be used as an example as the strategy, tasks and activities can vary depending on the country's objectives and current situation.

## *Recommendations*[54]

| No | Guideline | Details |
|---|---|---|
| 1. | **Plan, organise and deliver information security awareness initiatives appropriately** | Assess requirements and have a clear vision and set of objectives for the campaign. Planning makes the tasks and activities more manageable. Also create a communication plan. The whole end-to-end awareness-raising initiative should be an ongoing process e.g. re-educating or re-training targets from a previous awareness raising initiative (e.g. Denmark). |

[54] *Information security awareness programmes in the EU — insight and guidance for Member States*, ENISA, September 2006. The document is available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_is_aw_programmes_eu.pdf

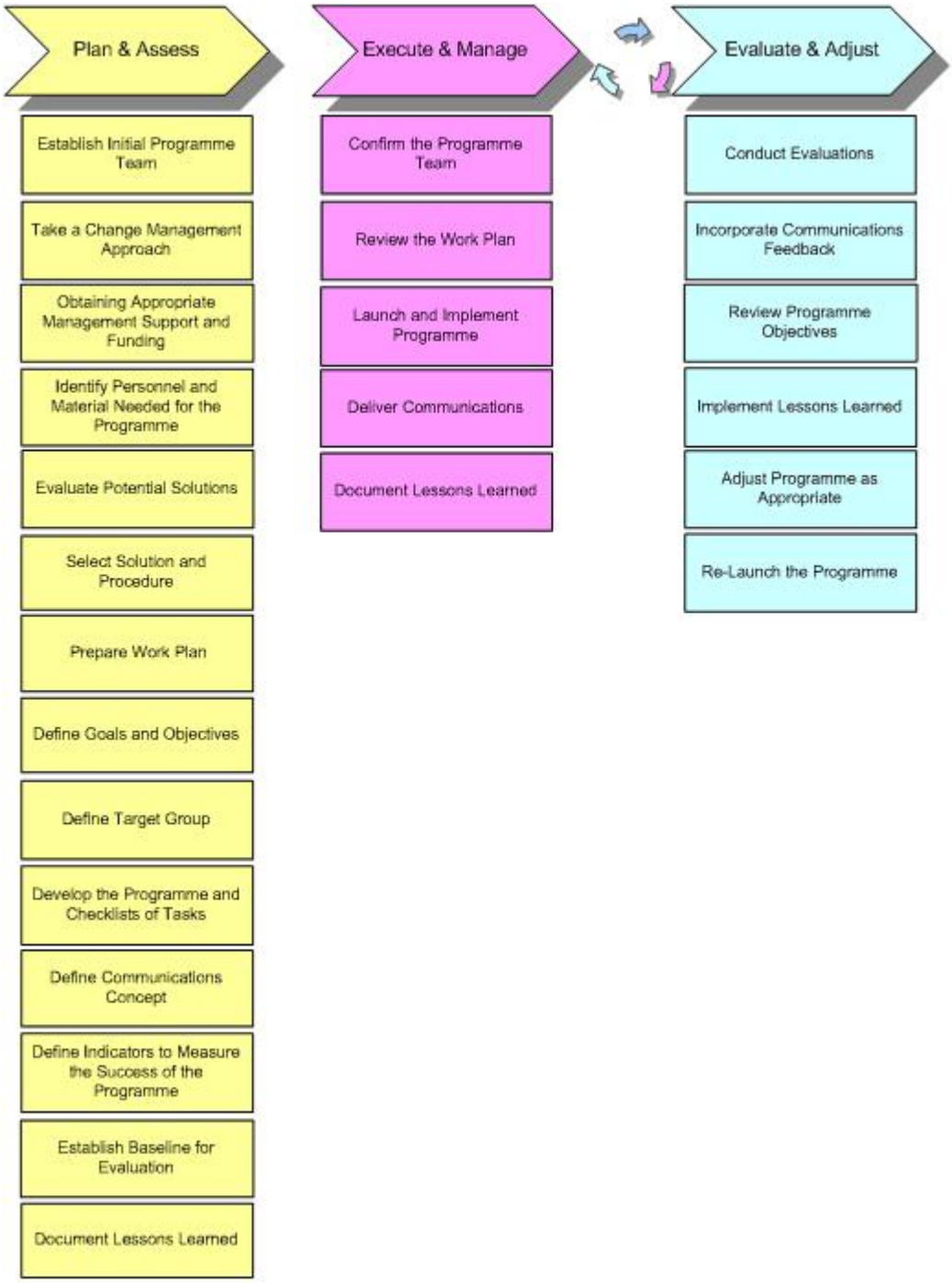
| | | |
|---|---|---|
| 2. | **Use different multipliers** | The media should be used as multiplier for the campaign. Other ways to utilise the multiplier effect include training trainers, informing teachers and working with ISPs (e.g. France, Italy, Luxembourg, Malta, the Netherlands). |
| 3. | **Utilise public–private partnerships** | Public–private partnership can be a highly effective way to deliver campaigns especially if each organisation can leverage strengths and resources. If a joint programme is developed, it is important to have codes of conduct and such elements as design guides (e.g. Ireland, the Netherlands). |
| 4. | **Collaborate with other organisations** | Working with other government departments or agencies can give more credit to any campaign (e.g. Italy, Malta, the UK). |
| 5. | **Use multiple channels** | It is important to use multiple channels to deliver the awareness-raising message; includes all online and offline medium (e.g. Spain). |
| 6. | **Use specific channels** | Using trade organisations, workshops, seminars and partner initiatives are all effective ways to target the audience of a programme. Specialist channels such as online computer sites or trade journals can be effective when targeting IT personnel due to the relevance to their day-to-day work. The use of agencies such as the local chambers of commerce, SME union networks, trade associations or business journals are all effective channels (e.g. Malta, Sweden, the UK).<br>Healthcare stations and social security institutions are effective ways to communicate with ‘silver surfers’ (e.g. Italy). |
| 7. | **Use effective channels** | With the abundance of online information, and with time often at a premium, using channels such as brochures, leaflets and fact sheets are very effective in getting attention and hence raising awareness (e.g. France, Germany, Lithuania, Spain). |

| | | |
|---|---|---|
| 8. | **Implement information security policies within the workplace** | Effective employee awareness can be achieved by the successful implementation of information security policies. These include the use of staff handbooks and manuals, contracts and letters of employment, induction exercises and training courses or ongoing on-the-job training (e.g. Finland, Germany, Sweden). |
| 9. | **Messages should be tailored and meaningful** | Content of messages delivered as themes or as usage scenarios can aid in perception and understanding. Also, different target groups may have different levels of understanding or expectations — the message delivered should be tailored and meaningful to the target group's interests, needs and knowledge levels (e.g. Finland, Norway, Sweden). |
| 10. | **Use a comprehensive set of computer-based training and communication tools** | An effective awareness-raising campaign to promote security awareness needs to be highly visible and understandable to all. One way is to dispel myths and incorrect assumptions or to show the target the error in their ways. Another way is to make the experience more interactive e.g. using web services on a website to test the strength of the target's password (e.g. Denmark, Finland, Italy, Luxembourg, Sweden). |
| 11. | **Identifying specific objectives and messages for each category of target group** | Where possible, the campaign message and channels used should be customised to the category level of the target group and be adapted to roles and responsibilities (e.g. Sweden). |
| 12. | **Create meaningful content** | Terms and definitions used should be meaningful and simple to understand to the intended target group (e.g. Germany, Italy, Norway). |

| | | |
|---|---|---|
| 13. | **Measuring programme effectiveness** | It needs to establish metrics to measure the performance of a campaign also establishing a baseline. Allows for lessons learned to be identified which can help increase the effectiveness of current or future initiatives (e.g. Denmark).<br>Conducting frequent surveys and reports during or after the campaign can help to fine-tune the channels used, message being delivered or overall success of the initiative. Also, it can be important to communicate the success stories, especially to the media (e.g. Denmark, Ireland). |
| 14. | **Raising awareness is not a one-off effort** | As there is continual change, an ongoing programme of security education or training is hugely important to raise awareness in employees on the risks to information security (e.g. Germany, Hungary, Italy, Lithuania, Netherlands, Sweden, the UK). |

## Checklists

When designing, implementing and executing any type of awareness-raising initiative, the tasks and activities required can be grouped into three main phases as follows[55]:




[55] For more information on any of the phases and subsequent checklist items, refer to *A user's guide: how to raise information security awareness*, ENISA, June 2006. The document is available at: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_a_users_guide_how_to_raise_IS_awareness.pdf

Breaking each phase down into tasks and activities, checklist items can be constructed. Member States should use these as guidance for the main steps to undertake when running any kind of information security awareness-raising programme:

## I. Plan and assess

| No. | Checklist item |
|---|---|
| 1. | ☑ **Establish initial programme team**: set up a programme team primarily for the first phase but with a view to transitioning them into subsequent phases (for continuity). Ensure roles and responsibilities clearly defined. |
| 2. | ☑ **Take a change management approach**: adopt and implement a change management methodology to ensure that the campaign objectives are reached and ultimately the target group's awareness and behaviour is changed. |
| 3. | ☑ **Obtain appropriate management support and funding**: get stakeholder/senior management buy-in and support. Look for public–private partnerships where possible. Cost benefit analysis can help when trying to identify funding needs and identifying programme benefits can help with getting buy-in and funding. |
| 4. | ☑ **Identify personnel and material needed for programme**: ensure programme team and resources sufficiently skilled and experienced, covering areas in IT, HR, communications and training and development. Utilise knowledge from Member States and other information repositories such as the Internet for identifying potential solutions. |
| 5. | ☑ **Evaluate potential solutions**: when evaluating potential solutions, consider public–private partnerships or whether the awareness programme can be planned and executed in-house or needs to be outsourced. |
| 6. | ☑ **Select solution and procure**: after careful evaluation, select the best solutions and organisations to implement the awareness programme. |
| 7. | ☑ **Prepare work plan**: start building a work plan and include the main activities for which the required resources, timescales and key milestones need to be identified. |
| 8. | ☑ **Define goals and objectives**: in order to effectively plan, organise and evaluate |

| No. | Checklist item |
|---|---|
| | an awareness programme, the programme goals and objectives need to be identified. |
| 9. | ☑ **Define target groups**: it is critical to identify and define the specific group that is targeted by the awareness initiative. Each target group has unique interests and needs, as well as operating in different environments. |
| 10. | ☑ **Define the programme and checklist of tasks**: efforts should be focused on designing the programme and on further developing and implementing the plan. Key messages should also be identified and developed. |
| 11. | ☑ **Develop communications concept**: an effective and efficiently implemented communication plan is critical to the success of an awareness programme. A strategy should be constructed identifying bodies/organisations that can be used as multipliers as well as which ones can be used as partners. The content of messages needs to be further developed and tested, and appropriate communication channels identified. |
| 12. | ☑ **Define indicators to measure the success of the programme**: in order to measure the performance of an awareness programme, it is imperative to clearly identify and construct metrics and key performance indicators. |
| 13. | ☑ **Establish baseline for evaluation**: apart from identifying metrics and key performance indicators, the current situation with regards to the target group needs to be understood. This way, the effectiveness of an awareness programme can be measured based on the change in landscape. |
| 14. | ☑ **Document lessons learned**: get the programme management and teams involved in capturing lessons learned from activities completed in the first phase. |

## II. Execute and manage

| No | Checklist item |
|---|---|
| 1. | ☑ **Confirm programme team**: before launching the programme, confirm the team that will be responsible for both execution and obtaining results. Each member of the awareness-raising team should have a specific role and set of responsibilities when implementing and managing the initiative. |

| No | Checklist item |
|---|---|
| | |
| 2. | ☑ **Review the work plan**: the work plan needs to be updated and programme milestones finalised. This has to be completed before launch, as the awareness-raising team need to be aware of, and comply with, the goals and objectives as well as budget requirements and project constraints. |
| 3. | ☑ **Launch and implement programme**: at this stage of the programme, all the protocols and arrangements should be in place and ready to go. The awareness-raising team and all partners should carry out any execution tasks or activities defined and assigned to them in the work plan. |
| 4. | ☑ **Deliver communications**: the communication plan should be implemented and associated messages delivered to the applicable target groups via the designed channels. As part of the metrics and key performance indicators, as well as capturing lessons learned, it is important to try to collect feedback on the communications. |
| 5. | ☑ **Document lessons learned**: repeat similar procedures to those used to capture lessons learned at the end of the first phase. Compare the historical evolution of the programme from a learning perspective. |

## III. Evaluate and adjust

| No | Checklist item |
|---|---|
| 1. | ☑ **Conduct evaluations**: in order to understand the performance of the programme and to try to quantitatively or qualitatively measure the effectiveness in raising information security awareness and hence reducing security incidents, data should be collected. Follow-up questionnaires and omnibus surveys are one way to conduct the evaluations. |
| 2. | ☑ **Incorporate communications feedback**: the feedback captured when delivering the programme's communications should be reviewed with a view to improving future plans. The information should be combined with the results derived from the evaluation metrics. |
| 3. | ☑ **Review programme objectives**: the success of an awareness programme can largely be decided by the outcomes in relation to the original objectives. If the programme is ongoing, then the original objectives may need to be revisited in |

| No | Checklist item |
|---|---|
| | light of the performance. |
| 4. | ☑ **Implement lessons learned**: the lessons learned from the previous phases combined with the feedback based on the communication plan, should be leveraged to make the ongoing or future programmes more effective. It is important to learn from both the successful and less successful activities. |
| 5. | ☑ **Adjust programme as appropriate**: if the programme is ongoing or to be re-launched, the experiences gained to date should provide knowledge and understanding to adjust the programme to make it more successful. Adjustments should be made while maintaining the focus on the programme goals and objectives. |
| 6. | ☑ **Re-launch the programme**: when re-launching the adjusted programme, tasks as identified in Phase II should be repeated. More effort should be funnelled towards those activities that maximise the effectiveness of the awareness-raising programme. |

## *Roadmap*

The following diagram illustrates how organisations and public bodies could outline and implement an awareness roadmap to help contribute to a culture of information security awareness. The diagram should only be used as an example as the strategy, tasks and activities can vary depending on the country's objectives and its current situation([56].

When reviewing the diagram, refer to the colour key below which aids to group together roadmap items.

| **Colour key**: | |
|---|---|
| | Roadmap item is typically done once and hence does not need to be continually undertaken. In some instances, the set of tasks and activities may be repeated but only in a minor capacity. |
| | Roadmap item is typically done in sequence and is ongoing from that point onwards. The set of tasks and activities are therefore continually performed after initiation. |
| | Roadmap item is typically done at the start, during and at the end of the awareness programme. The set of tasks and activities are therefore continually performed throughout the initiative lifecycle. |

[56] *Information security awareness programmes in the EU — insight and guidance for Member States*, ENISA, September 2006. The document is available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_is_aw_programmes_eu.pdf


| **Roadmap Item key**: |
|---|
| **Form public–private partnerships** (e.g. ranging from IT companies through to community organisations) |
| **Re-use material and knowledge** (e.g. use programme material and expertise from other Member States if applicable) |
| **Customise message and target home user/SME** (e.g. construct and deliver key target group-specific messages) |
| **Utilise primary channels** (e.g. develop and launch websites) |
| **Use multipliers** (e.g. leverage positions such as teachers that can reach a wider audience) |
| **Use media and ISPs** (e.g. collaborate with and use media and ISPs as communication channels) |
| |

| **Roadmap Item key**: |
| --- |
| **Enhance primary and develop secondary channels** (e.g. increase functionality of websites (making more interactive) or deploy other channels such as telephone hotlines) |
| **General training** (e.g. public events and awareness-training sessions for the general public) |
| **Customise message and target local government** (e.g. construct and deliver key target group-specific messages) |
| **Customise message and target ISPs** (e.g. construct and deliver key target group-specific messages) |
| **Specialist training** (e.g. classroom-based or train-the-trainer sessions covering role-specific functions) |
| **Alternative training** (e.g. e-learning training programmes) |
| **Translate material/message** (e.g. make campaign messages multilingual) |
| **Modify message and retarget all** (e.g. add to key messages covering topics such as WiFi or mobile phone security) |
| **Supplement message and retarget all** (e.g. add further detailed or organisation-specific messages) |
| **Analyse and fine-tune programme performance** (e.g. benchmark against baselines and use metrics and key performance indicators) |
| **Develop lessons learned and future direction** (e.g. compile recommendations and knowledge transfer) |