



## European Month of Network and Information Security for All – *A feasibility study*

November 2011





## About ENISA

The European Network and Information Security Agency (ENISA) is a European Union (EU) agency which acts as a centre of expertise for the EU Member States and European institutions. It gives advice and recommendations on good practice, and acts as a “switchboard” for exchanging knowledge and information. The agency also facilitates contacts between the European institutions, the Member States, and private business and industry.

## Contact details

To contact ENISA, or for general enquiries on information security awareness matters, please use the following details:

Isabella Santa, Senior Expert Awareness Raising – E-mail: [awareness@enisa.europa.eu](mailto:awareness@enisa.europa.eu)

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

## Acknowledgments

Several parties supported and contributed directly or indirectly to this work in a number of ways. ENISA wishes to acknowledge the efforts of the ENISA virtual working group members: Agustín López, Alexis Grammenos, Ana Teixeira Lopes, Andris Soroka, Andrzej Piotr Lewalski, Anke Gaul, Anthony Keane, Anton Tkachov, Arjen de Landgraaf, Brian Honan, Bruno Citarella, Bruno Morisson, Carlo Tyrberg, Claire Vishik, Claudio Telmon, David Prendergast, Diego Fernandez Vazquez, Fabrizio Cirilli, Francisco Moreno, François Thill, Frederik Kortbæk, Gabriella Biro, Gerasimos Ntouskas, Hans Pongratz, James Williams, João Martins, Johannes Wiele, Jordi Batlle, Jorge China López, Jorge Fernandes, Jorge Pinto, Josep Bardallo, Lambrecht Nieuwenhuize, Ljubomir Trajkovski, Luis Manuel Fernandez Simon, Mathieu Briol, Meltini Christodoulaki, Naresh Pankhania, Neil Stinchcombe, Olaf Jueptner, R. Niamat, Ralf Braga, Robert J. van Manen, Sharon Conheady, Sonia Valerio, Steven Furnell, Thomas Dallmann, Tim Harwood, Wendy Goucher and Zeina Zakhour who provided valuable inputs, material and prompt support for the compilation of this paper.

Finally, we would also like to acknowledge and thank the US Department of Homeland Security, the Directorate-General for the Information Society and Media at the European Commission and Insafe, who contributed to this document with informal reviews, valuable insights, observations and suggestions. The content would be incomplete and incorrect without their help.

## Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2011

# Contents

About ENISA	2
Acknowledgments	3
<b>1. Executive summary</b>	<b>6</b>
<b>2. Introduction</b>	<b>9</b>
2.1 Methodology	9
2.2 Definition	9
2.3 Purpose	9
2.4 Rationale and policy context	10
<b>PART 1: AN OVERVIEW OF NATIONAL SECURITY EVENTS ACROSS EUROPE</b>	<b>12</b>
<b>3. The European overview</b>	<b>13</b>
3.1 Security day/week	13
3.2 Summary of responses	13
3.2.1 Goals and objectives	14
3.2.2 Target group(s)	14
3.2.3 Subject matter	15
3.2.4 Type of messages used	16
3.2.5 Period when security days/weeks are organised	16
3.2.6 Languages	17
3.2.7 Delivery channels	17
3.2.8 Techniques	21
3.2.9 Costs	21
3.2.10 Measuring the effectiveness of awareness programmes	22
3.2.10.1 Other countries' experiences	23
<b>PART 2: ORGANISATIONAL INSIGHTS AND PATTERNS FOR THE 'EUROPEAN SECURITY MONTH'</b>	<b>24</b>
<b>4. Engaging Member States</b>	<b>25</b>
4.1. How to engage Member States	25
4.1.1 Why Member States should engage	25
4.1.2 Benefits for Member States	25
4.1.3 Endorse and support	26
<b>5. Engaging possible intermediaries</b>	<b>27</b>
5.1 Targeting intermediaries	27
5.2 Intermediary types	28
5.3 Endorsers and sponsors	30
5.4 The message	31
<b>6. Making a 'European security month' interesting</b>	<b>32</b>
6.1 Length of the campaign	32
6.2 Security topics	32
6.3 Communication concept	33

# CONTENTS

6.4 Targeted messages	34
6.4.1 <i>Vocabulary for the messages</i>	34
6.4.2 <i>Image for the messages</i>	34
6.5 Communication channels	34
6.5.1 <i>Availability of information</i>	35
6.6 Competitions	35
<b>7. Creating an identity</b>	<b>37</b>
7.1 Branding	37
7.1.1 <i>What is branding?</i>	37
7.1.2 <i>Why does the European Month of Network and Information Security for All need branding?</i>	37
7.1.3 <i>Other countries' experiences</i>	38
7.1.4 <i>Brand development recommendations</i>	39
<b>8. Capturing feedback and adjusting campaign objectives</b>	<b>41</b>
<b>9. A roadmap towards coordinated annual awareness efforts</b>	<b>42</b>
9.1 Alternative methods to jump-start EU awareness activities	45
<b>10. Organisation modalities</b>	<b>47</b>
10.1 Other countries' experiences	47
10.1.1 <i>Europe's experience</i>	47
10.1.1.1 Insafe's experience	48
10.1.1.2 US experience	49
<b>11. Conclusions</b>	<b>50</b>
<b>12. Appendices</b>	<b>51</b>
12.1 Appendix I – Inventory worksheet template	51
12.2 Appendix II – October 2010 NCSAM Proclamation	52
12.3 Appendix III – Endorsement Approval Form, National Cyber Security Awareness Month, October 2010	53
12.4 Appendix IV – Security awareness campaign topics	54
12.5 Appendix V – National Cyber Security Division (NCSD) organisational chart	56
<b>13. Index</b>	<b>57</b>
13.1 List of figures	57
13.2 List of tables	57
13.3 List of graphs	57



## EXECUTIVE SUMMARY



# 1. Executive summary

As part of its ongoing awareness raising mission, ENISA assesses the establishment and organisation of a European Month of Network and Information Security for All.

This concept was inspired by similar projects that have been held successfully in other places around the world for some years now. ENISA suggests that this project will significantly raise the awareness of EU citizens on Network and Information Security (NIS) issues. The particularities of the European territory compared to other areas of the world indicate that a significant amount of effort will be required in order for this idea to deliver its full potential across Europe. To this effect, one of the most critical elements for the success of this activity is to develop an effective structure and coordination scheme among participating entities.

This year, ENISA has been asked to assess the feasibility and explore various options on how such a campaign can become an effective instrument to raising awareness about NIS challenges and in particular:

- generate awareness about NIS,
- achieve long-lasting behavioural change,
- modify perception of risks,
- involve relevant stakeholders,
- disseminate security-relevant information.

To this end, a virtual working group was created to:

- gather information with regard to Member States' experiences on organising national security events held for one or more days or an entire week;
- compile these results and produce a European overview (as-is);
- assess feasibility by developing a coordination scheme and model;
- identify and eventually develop awareness material to be used during such a campaign.

The following did not qualify to be included in this analysis:

- any event organised under Safer Internet Day;
- programmes funded by the Structural Funds of the European Union and/or the European Commission;
- any event organised within an international project or international commemoration (e.g. International Youth Day);
- any conference, summit or forum organised for professionals only.

The report covers two main parts:

- the overview of the security-related days/weeks currently organised at national level across Europe;
- the organisational insights and patterns for delivering a European Month of Network and Information Security for All on annual basis.

The first part of the study looks at the current state of play in Europe. The main findings are:

- half of the Member States hold either a security day(s) or week(s);
- the majority focus was around security week(s) rather than day(s);
- the proportion of campaigns encompassing general users versus those targeting business users is almost the same;
- a wide variety of key messages are promoted across the different European countries;
- most of the events are organised in October and November, although many are organised in February and April;
- all supporting material and communication is produced in the official language of the countries concerned;
- printed materials (41 %) and electronic messages (36 %) are featured in many cases;
- websites are the most prominent channels of communication used (12 out of 15 Member States);
- all Member States used a variety of techniques that were fun, exciting and motivating;
- the public sector has been involved in the organisation of all the events that have been reviewed;
- messages should be tailored specifically to the audience and each intermediary;
- the wide variety of delivery channels used clearly demonstrates that there is no particular delivery method that has proven to be successful across all sectors and countries;

- the use of websites as a communication vehicle is followed by the use of magazines, brochures, documents, annual reports and other printed material (seven Member States) and events and meetings (seven Member States). Video clips and TV/radio/webcasts are two other common delivery channels.

The second part assesses the feasibility of delivering the European Month of Network and Information Security for All. The main findings are:

- leveraging on European and worldwide experiences would be essential – in particular Insafe could provide useful information of the success and challenges their previous campaigns and competitions have encountered;
- the implementation in coordination with the United States, where the cybersecurity month is established, is a supplemental model to jump-start the activities in Europe;
- engaging with relevant parties such as Member States and intermediaries is one of the most critical elements of this project;
- the involvement of the private sector would be required in order to deliver the full potential of this idea;
- an aim should be to broaden the scope of national security events to make them a solely international event;
- using appropriate communication channels and vocabulary will be critical for addressing multicultural aspects;
- branding will be key for the success of the 'European security month';
- a roadmap will be needed to provide a mechanism to help forecast developments and a framework to help plan and coordinate these developments. Member States might consider implementing one or more identified activities according to the level of engagement and information security awareness maturity of their country;
- alternative methods to jump-start the 'European security month' have been identified;
- one method appears to meet most of the requirements in relation to the organisation of a yearly security month across Europe. This method foresees three different phases: the production of a feasibility study; various activities and options of involvement and engagement of actors at national, European and global level; the implementation of a 'European security month' in all EU countries. The main features are:
  - the number and type of actors involved simultaneously;
  - the different type of proposed activities;
  - the various options of involvement and engagement open to the actors;
  - the timeframe foreseen for implementing coordinated annual awareness efforts.
- a structure would be essential to coordinate such a campaign across all Member States; the general principle of subsidiarity would apply;
- a decision-maker and someone to undertake the planning is essential, as well as national groups which should work to implement the 'European security month' activities at national level.

The analysis carried out in the study lead to the conclusion that organising a European Month of Network and Information Security for All is feasible especially because of the existing good practices and experiences of the Member States. This will be an annual activity, conducted in collaboration with the Member States and featuring a variety of national/European cybersecurity awareness raising initiatives and competitions.



## INTRODUCTION



## 2. Introduction

### 2.1 Methodology

ENISA created a virtual working group (VWG) to gather information with regard to Member States' experiences on organising national security events, and assess the feasibility with regard to the organisation of the European Month of Network and Information Security. The members of the ENISA VWG were volunteers drawn from the Awareness Raising Community members.

ENISA developed a questionnaire to be used by the ENISA VWG that focused upon gathering details about security-related days/weeks <sup>(1)</sup> currently organised at national level across Europe. Twenty-two Member States were targeted and all of them responded. The remaining countries did not receive the questionnaire because research and interviews conducted by ENISA had shown that these Member States did not organise any security event as defined in this report.

The inventory form <sup>(2)</sup> was aimed at extracting pertinent information in a way that was suitable to the responder. The questions and structure allowed for responders to control the format and size of the response without necessarily confining themselves. Whilst the priority of the form was the collection of material, the approach adopted also allowed responders the opportunity to present awareness-related initiatives as they perceive them.

This information has been quality checked with the relevant ministries and governmental agencies and in some cases supplemented by additional material, interviews and research carried out by ENISA centrally.

Data has been aggregated by combining data elements from different sources to provide insights and identify patterns in the organisation of security events across Europe and behaviours of the general public.

### 2.2 Definition

The report refers to security days/weeks that focused upon specific information security topics (e.g. data protection, e-safety) and in which dedicated events are organised to raise security awareness of specific target groups. The events are arranged at national level and eventually deployed regionally.

### 2.3 Purpose

The purpose of this document is, therefore, to carry out a feasibility study containing an analysis by examining the possible implementation of a 'European security month' in addition to an overview of the prevailing elements of security days/weeks organised at national level across Europe.

The overview primarily consists of the information supplied by Member States (i.e. ministries, governmental agencies or other organisations). This report also includes good practice recommendations and offers guidance on organising the European Month of Network and Information Security for All. A roadmap has also been developed to show a holistic progression towards coordinated annual awareness raising events.

This paper should not be seen as a comprehensive source of information of all security events that have been undertaken in Europe; the analysis is based on data provided by the Member States, organisations and public bodies and gathered through interviews and research.

Events organised at national level to celebrate Safer Internet Day did not qualify for inclusion in the analysis as they provide a range of information, awareness raising tools and educational resources on issues relating to online safety for parents, teachers, children and young people only <sup>(3)</sup>. Nor did other programmes funded by the Structural Funds of the European

<sup>(1)</sup> Security day/week refers to any event organised for one or more days or one or more weeks.

<sup>(2)</sup> The inventory worksheet template is presented in Appendix I.

<sup>(3)</sup> Safer Internet Day is organised by Insafe each year in February to promote safer and more responsible use of online technology and mobile phones, especially amongst children and young people in more than 70 countries from across the world. Insafe is co-funded by the European Union. More details are available online (<http://www.saferinternet.org/web/guest/home> and <http://www.sidfair.org>) (last accessed 28 June 2011).

Union and European Commission (i.e. INHOPE) <sup>(4)</sup>, international projects, portals, hotlines, conferences, summits and forums organised for ICT professionals, which were excluded on similar grounds due to a high degree of specificity.

## 2.4 Rationale and policy context

This section provides selected information and facts that motivate and explain the decision to explore the possibility of organising a European Month of Network and Information Security for All. The main aiming of this NIS month includes:

- promoting safer use of the Internet for all users;
- raising visibility of both networks through high-profile European events, and strengthening their identity by striving for common goals and setting up joint actions;
- building a strong track record to raise awareness through the 'European security month';
- increasing national media interest through European and international dimension of the project;
- enhancing attention and interest on information security through political and media coordination.

Since 2005, the Commission <sup>(5)</sup> has highlighted the urgent need to coordinate efforts to build trust and confidence of stakeholders in electronic communications and services. To this end a strategy for a secure information society <sup>(6)</sup> was adopted in 2006.

On 30 March 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacks and cyber disruptions: enhancing preparedness, security and resilience' <sup>(7)</sup>, setting out a plan (the 'CIIP action plan') to strengthen the security and resilience of vital Information and Communication Technology (ICT) infrastructures. The aim was to stimulate and support the development of a high level of preparedness, security and resilience capabilities both at national and European levels. This approach was broadly endorsed by the Council in 2009 <sup>(8)</sup>.

In the context of the CIIP action plan, the Commission discussed and developed European principles and guidelines for the resilience and stability of the Internet ('the Principles') <sup>(9)</sup>. In particular, the European Commission states that '*Public authorities, with the support of other stakeholders, as appropriate, should strive to educate and raise awareness on the risks associated with Internet-related activities.*

It is recognised that certain categories of stakeholders are not always in a position to properly understand the risks – both for themselves and for the stability and resilience of the Internet as a whole – associated with their Internet-related activities.

Without prejudice to the competences of Member States in the area of culture and education, and taking in the utmost account the principle of subsidiarity, a shared EU approach to such activities, with a view to achieve a global approach, should be sought.

The private sector has an important role to play in supporting public authorities and in providing clear information to all stakeholders, concerning the potential risks of their behaviours for the stability and resilience of the Internet, e.g. unwillingly propagating virus and other malware, having their computers enrolled in a Botnet, etc.

*Strengthening education efforts in this area will also have the benefit of producing skilled experts in the needed ICT fields. Education and awareness-raising will also strengthen the preventive abilities of stakeholders, which in turn will help to avoid recourse to ex post or overly invasive security measures' <sup>(10)</sup>.*

<sup>(4)</sup> INHOPE is the International Association of Internet Hotlines. More details are available online (<http://www.inhope.org>) (last accessed 10 June 2011).

<sup>(5)</sup> COM(2005) 229.

<sup>(6)</sup> COM(2006) 251.

<sup>(7)</sup> COM(2009) 149.

<sup>(8)</sup> Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security (2009/C 321/01).

<sup>(9)</sup> European principles and guidelines for Internet resilience and stability ([http://ec.europa.eu/information\\_society/policy/nis/docs/principles\\_ciip/guidelines\\_internet\\_fin.pdf](http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf)).

<sup>(10)</sup> European principles and guidelines for Internet resilience and stability ([http://ec.europa.eu/information\\_society/policy/nis/docs/principles\\_ciip/guidelines\\_internet\\_fin.pdf](http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf)).

On these lines, the Digital Agenda for Europe (DAE) <sup>(11)</sup>, adopted in May 2010, and the related Council conclusions <sup>(12)</sup> highlighted the shared understanding that trust and security are fundamental preconditions for the wide uptake of ICT and therefore for achieving the objectives of the 'smart growth' dimension of the Europe 2020 strategy <sup>(13)</sup>. The DAE emphasises the need for all stakeholders to join their forces in a holistic effort to ensure the security and resilience of ICT infrastructures, by focusing on prevention, preparedness and awareness, as well as to develop effective and coordinated mechanisms to respond to new and increasingly sophisticated forms of cyber-attacks and cybercrime. This approach ensures that both the preventive and the reactive dimensions of the challenge are duly taken into account.

These documents provide the rationale and policy context for discussion and cooperation with the Member States and international organisations and, where appropriate, with private sector organisations with the objective to assess the feasibility of organising a security month in Europe, possibly in coordination with the United States.

Finally, the suggested guidelines foresee the full use of ENISA, as well as other bodies (e.g. the Member States, the Commission and/or industry), to map the 'Principles' into more concrete and operational activities.

---

<sup>(11)</sup> COM(2010) 245.

<sup>(12)</sup> Council conclusions of 31 May 2010 on Digital Agenda for Europe (10130/10).

<sup>(13)</sup> COM(2010) 2020 and conclusions of the European Council of 25/26 March 2010 (EUCO 7/10).



## **PART 1: AN OVERVIEW OF NATIONAL SECURITY EVENTS ACROSS EUROPE**

## 3. The European overview

### 3.1 Security day/week

All countries across Europe <sup>(14)</sup> have been asked to provide information regarding any event organised to raise citizens' information security awareness at national level and eventually deployed regionally (i.e. an event organised for one or more days or one or more weeks).

### 3.2 Summary of responses

The report analyses how governments and organisations within the European Union (EU) and the European Economic Area (EEA) countries are approaching information security awareness by organising security events (i.e. day/week) to educate citizens on the importance of implementing effective information security practices throughout the year.

The responses refer to the most recent and successful national events organised either by the government or a public body of a country solely or by a public-private partnership. When it was not possible to report about any event other than one organised by a private company, this data has been included (one EU Member State).

Data for a total of 127 events were gathered and analysed across 22 countries. When a security event was organised for the entire year, a total of 12 events per country were counted (Belgium, Spain, Italy, the Netherlands and Sweden).

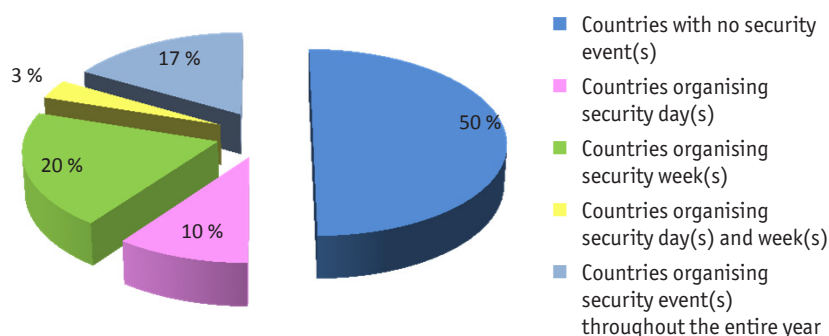
The survey carried out by ENISA reported that 14 EU Member States organise such events; while one out of three EEA countries does organise them.

These 15 countries could be divided between geographical zones as follows: 40 % in northern Europe; 40 % in central Europe and 20 % in southern Europe. The experience in organising such events varies from one country to another. In 2010–11, Belgium and Slovenia organised their first security days/week, while the Netherlands held their first in 2003, Sweden in 2002 and Austria in 1997. Overall, 67 % of the Member States that organise security events started before 2008. On average EU Member States have been running a security themed day/week for 5.4 years. There are big national differences, reflecting the 'digital divide' between people in different countries and regions.

Overall, only 10 % of the Member States organise security days: of these, only one country organised activities for one day only, while the others hold events for two or three days. The majority of countries (20 %) organise security weeks <sup>(15)</sup>, and the remaining countries (3 %) organise both. Five countries (17 %) primarily organise events throughout the entire year <sup>(16)</sup> (Figure 1).



Figure 1: European overview



<sup>(14)</sup> EU Member States and EEA countries.

<sup>(15)</sup> Of these nine countries, four organise security events for a minimum of an entire month to a maximum of 11 months.

<sup>(16)</sup> This refers to initiatives that operate periodically or on an ongoing basis throughout the entire year.

### 3.2.1 Goals and objectives

All over the EU, security events are aimed at informing users about the importance of information security and highlighting the simple steps people can take to protect their data, whether personal, financial and/or professional. Raising awareness, changing behaviour and providing resources to all citizens about how to protect themselves online were the main goals and objectives reported.

### 3.2.2 Target group(s)

Almost all countries reported events organised for ‘all’, ‘individuals’, ‘citizens’ or ‘the general public’. Only a few reported to have run a campaign for a very specific target group, such as 13- to 18-year- old students, parents, etc.

Examples of groups that have been targeted by information security days/weeks across Europe are listed below <sup>(17)</sup> (note that the specific names presented here are as provided by the respondents from the Member States, so the groups are not distinctive):

- 13- to 18-year-old students
- adults
- citizens
- companies
- consumers
- educators
- government institutions
- home users
- Internet users, primarily aged 25 and older
- IT civil servants
- IT professionals (e.g. IT managers, CIO, security engineers)
- kids
- parents
- public administrations.
- schools
- Small Medium Enterprises (SMEs)
- teenagers
- young children

Given the clear overlap between some of the reported groups, it is useful to group similar audiences into three broader categories: general users, young people and business users, as shown in Table 1.

<sup>(17)</sup> The information is listed in alphabetical order.



**Table 1:** Categorisation of the target groups

Main category	Target group
General users	citizens
	consumers
	parents
	educators
	adults
	home users
	Internet users, primarily aged 25 and older
Young people	kids
	young children
	teenagers
	13- to 18-year-old students
	schools
Business users	SMEs
	IT professionals
	IT civil servants
	companies
	government institutions
	public administrations

The proportion of campaigns encompassing general users versus those targeting business users is almost the same. This is due to the numerous campaigns targeting SMEs. The number of these events is approaching the one targeting ‘citizens’. By contrast, the number of security events specifically for young people is about half the number dedicated to general users.

It is worthwhile emphasising the need to define better the specific audience that is targeted by the awareness initiative in order to tailor the message content to the target group’s knowledge or technical aptitude using the most effective communication channels. This will maximise the appeal of the message and persuade the audience to take action, especially if the message fits with the target group’s interests and needs.

### 3.2.3 Subject matter

The analysis carried out by ENISA reported that the security topics most often addressed by the national security events across Europe were:

- Internet safety <sup>(18)</sup>
- identity theft
- privacy
- passwords
- phishing
- fraud and cybercrime
- cyber-bullying
- social networks
- wireless access
- social engineering
- encryption
- shredding and secure disposal.

<sup>(18)</sup> This refers to security events different from those organised for celebrating the Safer Internet Day.

Some of these topics were more dominant than others, e.g. Internet safety, identity theft, privacy, passwords, phishing and fraud. It is clear that most of the themes identified can have potential relevance to EU citizens in the context of their business and personal lives.

## 3.2.4 Type of messages used

It has not been possible to categorise the messages used in the European countries, mainly because of the variety of style and languages used.

However, data confirm that there is a need to define better the message used to target the audience. This will maximise the appeal of the message and persuade the audience itself. The message should be proactive, topical for the target group and consistent.

Data show that slogans have been created to better promote security events in some countries and increase the level of recognition that citizens have of a particular awareness security project and its specific activities. Creating a meaningful and possibly inspiring phrase is shown to be good practice across Europe and worldwide. The US Department of Homeland Security (DHS), for example, created – in coordination with industry – the slogan ‘Stop. Think. Connect.’ for its multi-year National Cyber Security Awareness Campaign. In addition, it uses the phrase ‘Our Shared Responsibility’ as the tag line for National Cyber Security Awareness Month (NCSAM).

Within the same campaign, different security tips can be used. Every tip can contain different advice as shown in Table 2 <sup>(19)</sup>.

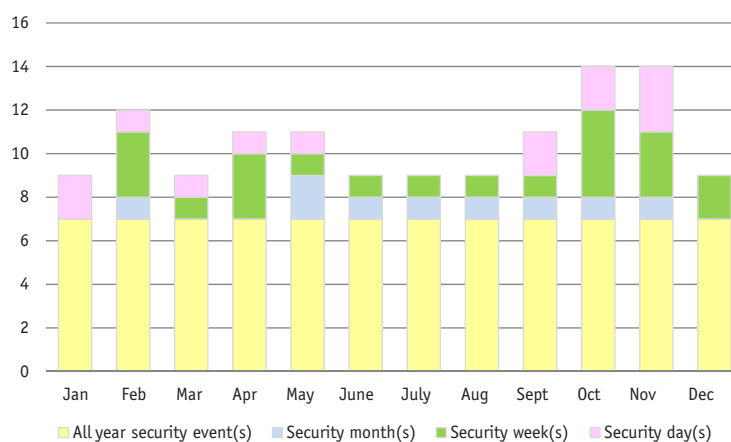
**Table 2:** Security tips

Tip	Advice
Protect your personal information	Secure your accounts
	Make strong passwords
	...
Keep a clean machine	Keep security software current
	Automate software updates
	Protect all devices that connect to the Internet
	...

## 3.2.5 Period when security days/weeks are organised

Graph 1 provides an overview of the spread of security days/weeks through the year, as currently organised across Europe.

**Graph 1:** Month(s) when security event(s) are organised



<sup>(19)</sup> More details are available online (<http://www.stopthinkconnect.org/tips.html>).

Graph 1 shows that 28 events are organised in October and November, 12 in February, followed by those organised in April, May and September. The organisation of Safer Internet Day in February explains why events have remained markedly scheduled in this period. An additional observation to make relates to the seasonality of events, with fewer events tending to fall in the summer period – an average of nine events per month as opposed to an average of almost 11 across the rest of the year.



### 3.2.6 Languages

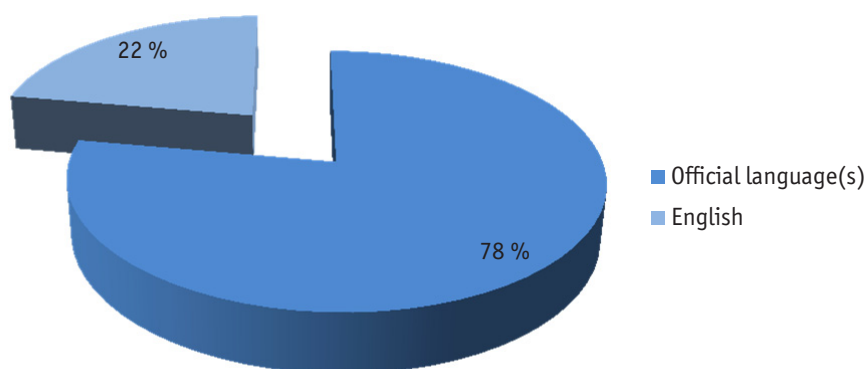
The European Union has 23 official languages: Bulgarian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish.

Figure 2 provides information on the languages used during the security day/week. The main challenge for a few Member States has been to develop an approach that is suitable for all citizens speaking several different languages. To counteract this, the Member States engaged themselves in building suitable training plans and materials in more than one language. To create the greatest impact on citizens, materials were available in the official language of the countries concerned (78 %); Figure 2 also confirms the tendency of some Member States to produce material in English as well (22 %). Two of these countries produced their documentation in other languages too: Ireland produced material in Mandarin and Polish; Finland in Swedish.

Similarly, in the United States, all content on the 'Stop. Think. Connect.' website (<http://www.stopthinkconnect.org/>) has been translated into several languages, for example French, German, Portuguese and Spanish.

The choice of the language is very important: most of the countries used their national language(s) during the entire duration of the events but some used English as well. This demonstrates that to make messages effective, it is key to use the national language(s). In future, any material produced for the European Month of Network and Information Security for All shall be ideally available in all 23 official languages taking into consideration that slogans and messages that are very effective in one country may be completely inappropriate in another. The involvement of Member States and intermediaries in general would be key to engage the right stakeholders to address this matter.

Figure 2: Languages used



### 3.2.7 Delivery channels

ENISA identified 21 delivery channels that have been used to some degree across Europe <sup>(20)</sup>:

- websites
- magazines, brochures, documents, annual reports and other printed material

<sup>(20)</sup> The information is listed in order of popularity.

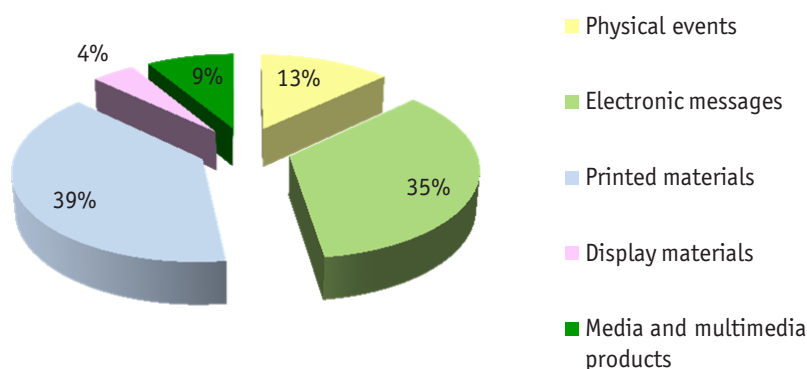
- conferences, seminars, workshops, summits, events, meetings, presentations
- TV, radio, webcasts
- video clips
- flyers, leaflets
- comics
- postcards, stickers, badges
- newspaper articles
- online games
- posters
- social networks
- advertisements
- books, guides
- e-mail
- exhibitions, expos
- merchandising (e.g. toothbrush)
- newsletters
- roadshows
- SMS
- tests, quizzes.

The wide variety of delivery channels used clearly demonstrates that there is no single delivery method that has proven to be successful across all sectors and countries. It also suggests the potential value of a multifaceted approach that can match different messages to different media and opportunities.

Different colour codes have been used for grouping the different delivery channels in broader categories, based upon the type of message involved: physical events (yellow), electronic messages (light green), printed materials (light blue), display materials (pink) and media and multimedia products (green). While some cases (e.g. newsletters) could be electronic or printed, the likelihood is probably the latter as the distribution mechanism to do it electronically would presumably have been classed as e-mail or web.

Figure 3 shows the broad percentages for the delivery categories that were identified. Printed materials (39 %) and electronic messages (35 %) feature in many cases.

**Figure 3: Grouping of delivery channel(s)**



The analysis carried out by ENISA reported that, within the top delivery channels used to make citizens aware of security issues, websites, magazines/brochures etc., conferences/seminars/workshops etc., video clips, TV/radio/webcasts, and flyers/leaflets are the most common as illustrated in Graph 2.

According to the analysis carried out by ENISA, one country reported using just one delivery method (i.e. TV/radio/webcasts), seven countries use two to four channels and seven countries use more than five.

In particular, the majority of Member States (12) which run either a security day or week used a website as the main channel of communication with their target group. This analysis shows that the best tool for conveying a consistent message over time is a website: the website is the backbone of ongoing communications and is beneficial to gain feedback following which adjustments can be made to the various approaches. Moreover, a website can present content for multiple audiences, is easy to update and maintain, can be easily linked to other information and can be integrated with more than one delivery channel, for example radio, webcast and e-mail. Developing a website is probably one of the least expensive and most efficient methods of communication. Directing the audience to the website is one of the key challenges to ensuring its success and will require the support of many other public and private sector organisations in every country to advertise and support it.

Websites, as a communication vehicle, are followed by magazines, brochures, documents, annual reports and other printed material (seven Member States) as well as by events and meetings (seven Member States). Within brochures and magazines, it is easier to define message content and format to reach an established audience. Events and meetings create high impact and can reach a very wide range of audiences by careful selection of venues and topics. This delivery channel has more chance of interesting the audience due to the interactive element of the channel.

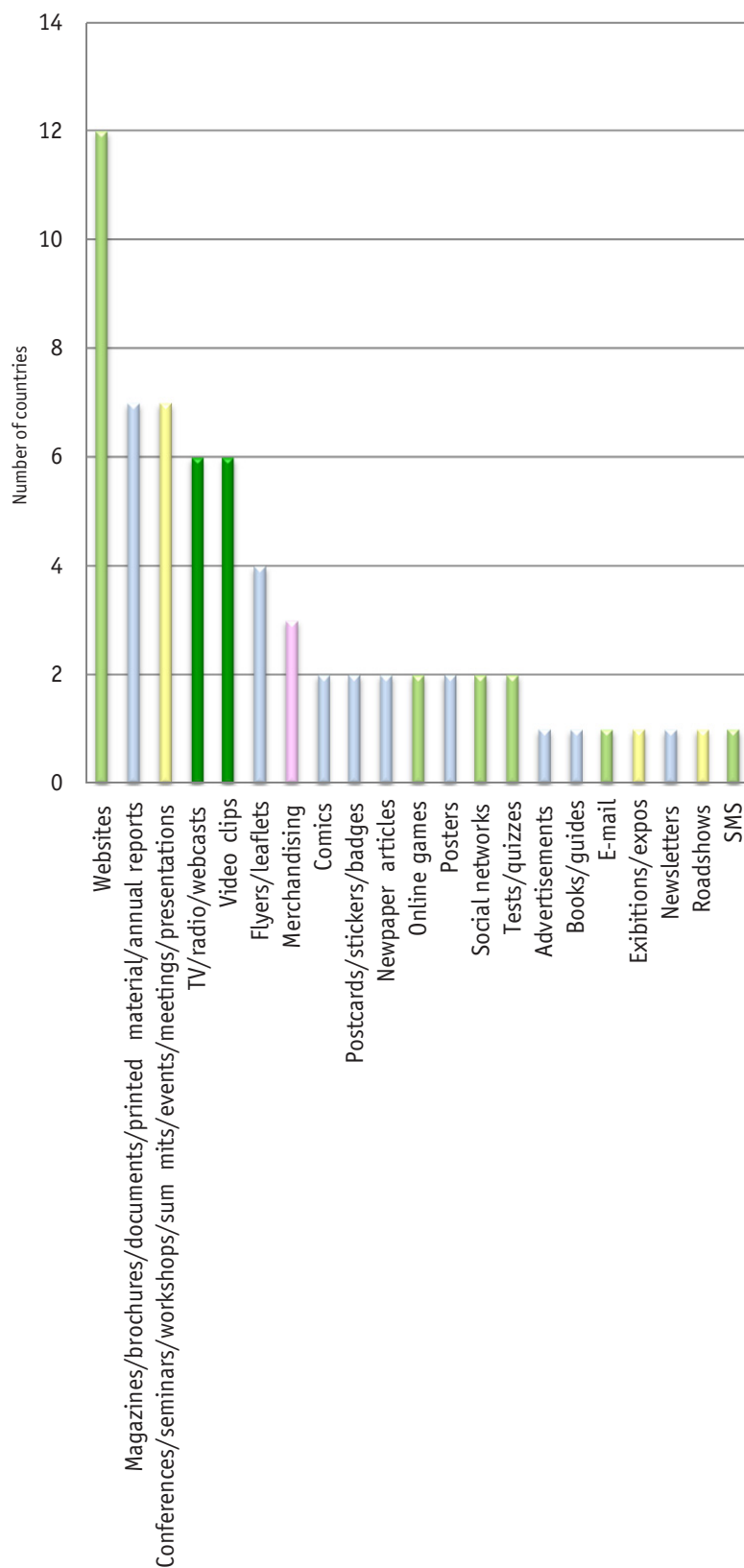
Finally, video clips (six Member States) and TV/radio/webcasts (six Member States) are two other common delivery channels used across Europe by countries running a security event.

Video clips are one of the most common delivery channels used by Member States. Research conducted by ENISA and statistics on the download of the ENISA video clips available at the ENISA website show that videos work well for groups of any size and also provide an easy way to allow users to replay the message numerous times. It is important that video clips are designed for the specific audience. Custom-made clips can be very effective, although expensive to produce. To help the Member States and provide a common framework, the ENISA video clips will be available in all 23 official languages.

TV/radio/webcasts can create high impact. This delivery channel comes as close as any medium can to face-to-face communication. In some cases, the personal message delivered by an authority can be very convincing. TV and radio offer audience selectivity by programming. They offer scheduling flexibility of different programmes and times of day and the opportunity to stress reach or frequency. The experience of Luxembourg, for example, demonstrates how successful and effective the use of radio spots could be in the context of information security events; the preferred delivery channel for Belgium is the use of webcast and radio.

Surprisingly, posters are not used so often during security events organised across Europe.

Graph 2: Delivery channel(s)





### 3.2.8 Techniques

In general, all Member States used a variety of techniques which were fun, exciting and motivating. Ways used to make information security events interesting included:

- the use of analogies;
- the use of easy-to-understand terms;
- the use of different messages and activities to ensure awareness was always fresh;
- the use of practical messages;
- the organisation of memorable activities.

### 3.2.9 Costs

The questionnaire did not include a section related to either the fixed or variable costs connected to the organisation of national awareness initiatives across Europe. This is because costs vary greatly from one country to another depending on the number of events organised, material produced, the availability of resources, previous projects, etc. For example, many countries reported the use of the same delivery channels as a method to disseminate their messages: one reason is that the costs can be contained. Considering all these variables and, in particular, the complexity of the campaign organised and its duration, it would not be possible to calculate the average total budget request for a network and security campaign organised in Europe.

However, ENISA indicated in a recent report that, although the costs will vary greatly from one security campaign to another depending on their structure, availability of assets and so forth, the main expenses will be incurred by the information security awareness programme team <sup>(21)</sup>. Table 3 provides some of the most common cost elements for information security awareness initiatives, including illustrative cost estimations based on actual figures given from an airline corporation <sup>(22)</sup>:

**Table 3:** Cost estimations based on actual figures given from an airline corporation

Cost	Description	€ Estimate
<b>Personnel</b>	Personnel working on the information security awareness initiative. Whether they are full or part-time depends largely on the size of the organisation and the importance of information security relative to other priorities.	60 000
<b>Operational Costs</b>	The operational costs include rent, website maintenance – extranet and intranet –, information security awareness materials – posters, briefing papers, office miscellaneous costs.	25 000
<b>Advertisement and Promotion</b>	Branded coasters, pens, prizes for information security tests, quizzes and competitions, coffee for brown-bag meetings and so on.	Promo material cost
		Promo distribution cost
		Advertisement creative cost
		Advertisement media cost
<b>Training</b>	In the event an organisation organises awareness training sessions.	Individual materials cost
		Training rooms cost per session
<b>Contingency</b>	Further funds may be needed to purchase additional security awareness materials, external training courses and so on.	100
<b>Total budget request</b>		20% on total
		<b>TOTAL</b>

Another element, which would be useful when trying to create and advise on campaigns for different Member States, is the costs associated with the delivery channels based on an analysis conducted by the ENISA VWG.

<sup>(21)</sup> *The new users' guide: How to raise information security awareness*, ENISA, November 2010 (<http://www.enisa.europa.eu/act/ar/deliverables/2010/new-users-guide>) (last accessed 11 May 2011).

<sup>(22)</sup> *Obtaining Support and Funding from Senior Management*, ENISA, 2008 (<http://www.enisa.europa.eu/act/ar/deliverables/2008/obtaining-support>) (last accessed 19 October 2011); *Business case for an Information Security Awareness Program*, Noticebored, 2008 ([http://www.noticebored.com/NB\\_generic\\_business\\_case\\_for\\_infosec\\_awareness\\_program.pdf](http://www.noticebored.com/NB_generic_business_case_for_infosec_awareness_program.pdf)) (last accessed 17 October 2011).

The estimated costs take into consideration the ‘reach out’ and return on investment of different approaches. For example, while a website might cost more to produce than a poster, it is likely to have considerably more potential to reach a wide audience. So, the ‘cost per informed citizen’ as a result would be significantly less.

Similarly, the message potential of each channel will differ. The volume of information that could be conveyed within an advert or a poster would be much less than in a guide or a website.

### 3.2.10 Measuring the effectiveness of awareness programmes

Many business leaders have observed that ‘what gets measured, gets done’. Ultimately, information security awareness is about people’s behaviour. This is always hard to measure, so this is a challenging area for most countries.

Different Member States adopted different methods to assess the effectiveness of information security awareness activities <sup>(23)</sup>. In general, ENISA did not receive any empirical data but has collected some anecdotal evidence on how Member States measure the effectiveness of awareness programmes. There is a little consensus among respondents on the most effective measures. This is clearly an area where good practice is evolving. Generally, the data which have been gathered, and the research conducted, did not show significant differences between the European countries. This indicates that what people have found effective is broadly similar. Table 4 illustrates different performance indicators that have mostly been used across Europe.

**Table 4:** Performance indicators used across Europe

No	Performance indicator	Approach
1	Number of materials distributed/month	Process improvement
2	Number of materials distributed/edition	Process improvement
3	Number of events listed/month	Process improvement
4	Number of people attending awareness events per campaign	Process improvement
5	Number of visitors to a website/month	Process improvement
6	Number of downloads/video clip	Process improvement
7	Mean time between discovery and notification of an attack and/or new threat	Attack resistance
8	Number of security incidents/month	Efficiency and effectiveness
9	Average cost of security incidents per user	Efficiency and effectiveness
10	Cycle time in days between upgrade of antivirus and its use	Internal protections
11	...	...

Each performance indicator can be redirected to a different approach <sup>(24)</sup>.

- ✓ **Process improvement:** this approach assesses the effectiveness of the campaign by looking at its activities. These measures are easy to define and gather: however, they do not directly measure whether the end result has improved security.
- ✓ **Attack resistance:** this approach measures how resistant users are to a potential attack. This approach provides evidence on the level of awareness of the people concerned. However, the number of attack scenarios is quite high, and the measure will be specific to the scenario it is testing.
- ✓ **Efficiency and effectiveness:** this approach focuses on the actual experience of security incidents. The data can be gathered through the overall security incident but does not necessarily give a true reflection of security awareness. It is not just awareness that determines whether incidents occurred. However, in the long term, the trend can be a good indicator of awareness.
- ✓ **Internal protection:** this approach assesses how well users are protected against threats. The advantage of these measures is that they provide direct evidence of users’ behaviour. Often, though, the campaigns are aiming to change behaviour. This can result in many metrics.

<sup>(23)</sup> *The new users’ guide: How to raise information security awareness*, ENISA, November 2010 (<http://www.enisa.europa.eu/act/ar/deliverables/2010/new-users-guide>) (last accessed 11 May 2011); *Information security awareness initiatives: Current practice and the measurement of success*, ENISA, July 2007 (<http://www.enisa.europa.eu/act/ar/deliverables/2007/kpi-study/en>) (last accessed 11 May 2011).

<sup>(24)</sup> *Information security awareness initiatives: Current practice and the measurement of success*, ENISA, July 2007 (<http://www.enisa.europa.eu/act/ar/deliverables/2007/kpi-study/en>) (last accessed 11 May 2011).

### 3.2.10.1 Other countries' experiences

Table 5 shows the indicators used to assess the success and impact of the National Cyber Security Awareness Month (NCSAM) in the United States.

**Table 5:** Indicators used to assess the success of the NCSAM in the United States

No	Indicator
1	Number of events the leadership attends during the US National Cyber Security Awareness Month (supported by the Outreach and Awareness (O & A) programme)
2	Number of hits on the 'Stop. Think. Connect.' website
3	Number of campaign 'Friends'
4	Number of states issuing a proclamation <sup>(25)</sup>
5	Number of states and federal agencies hosting a NCSAM event

<sup>(25)</sup> A copy of the NCSAM proclamation is presented in Appendix II.



## **PART 2: ORGANISATIONAL INSIGHTS AND PATTERNS FOR THE 'EUROPEAN SECURITY MONTH'**

## 4. Engaging Member States

### 4.1 How to engage Member States

Half the European countries organise national security events relevant to their territory. ENISA believes that engaging Member States is one of the most critical elements of this project.

One option is to collaborate with the organisers of these existing events and aim to broaden the scope to make events more international rather than purely national. The United States has already designated October as its National Cyber Security Awareness Month, and Europe has organised its Safer Internet Day for February. The US Department of Homeland Security (DHS), the National Cyber Security Alliance (NCSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), the primary drivers of NCSAM, coordinate during October to highlight what home users, schools, businesses and governments need to do in order to protect their computers, children, and data. A possible collaboration with the United States or Insafe – the European network of Awareness Centres promoting safe, responsible use of the Internet and mobile devices to young people <sup>(26)</sup> – would be seen as an advantage for the success of a European security event. If not entirely conducive, they may at least be able to provide useful information on the successes and challenges of their previous campaigns. This would enable the organisers to benefit from case studies of previous campaigns which would illustrate the success factors and challenges encountered. Other primary considerations would be to explain why Member States should engage, to illustrate the benefits and terms for support and funding, and to analyse the advantages and disadvantages of running such an event.

#### 4.1.1 Why Member States should engage

The cyberspace is a shared resource and making it secure is a shared responsibility. No individual, business, or government entity is solely responsible for securing it. Everyone has a role to play in securing their part of cyberspace, including the computers, devices and networks they use. The general public needs to understand how individual actions have a collective impact on cybersecurity and its protection, and the Member States could help in ensuring this.

The actions which might be taken may differ. However, if each Member State does its part, whether by raising awareness in the community, educating young people or training users, together, all countries will become more resistant and resilient.

#### 4.1.2 Benefits for Member States

Having a centrally organised 'European security month' would have several benefits for the Member States involved: some of these are illustrated in Table 6.

**Table 6:** Benefits of the European Month of Network and Information Security for All

Benefits	
	Description
<b>Increase impact and visibility</b>	A European-wide project would create a greater impact and receive more attention from both national and international media
<b>Increase efficiency</b>	The principle of economy of scale would apply
<b>Use of ready-to-use material</b>	Material produced by third parties such as ENISA, the DHS or other Member States could be used across Europe to ensure a consistent message is delivered
<b>Reduce costs/investments</b>	A European-wide project would mean that the very best minds and experience from across the Union could be gathered together, thus reducing cost and required investment from each stakeholder

The coordination of the project at European level, rather than at a national level, would guarantee a consistent approach and message in all participating countries whilst allowing for national/cultural flexibility. This, in turn, could result in creating more impact, better results and more extensive media coverage.

In this regard, media coverage would affect the extent of information dissemination as well as influence audience opinion when communicating the information. Positive media coverage could help create a better image and positive public opinion.

<sup>(26)</sup> <http://www.saferinternet.org/web/guest/about-us> (last accessed 3 May 2011).



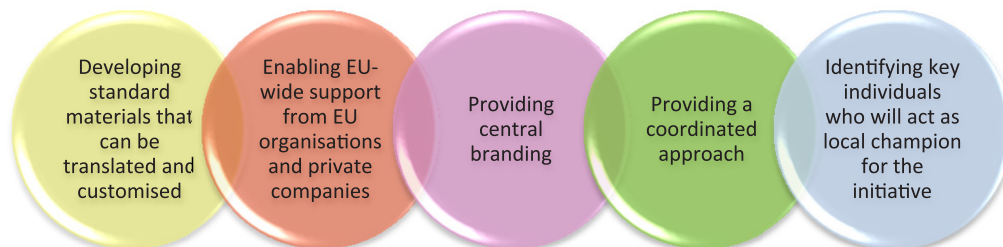
ion. Different types of media coverage could be defined based on two important elements — the type of mass media used and the style of coverage. There are numerous types of media coverage.

- Television coverage refers to the presentation of news or information or views on television. Television news channels are the primary source of media coverage.
- Radio coverage involves broadcasting news, information or entertainment via radio. Nowadays, the popularity of this medium has declined.
- Newspaper coverage refers to providing news, information or infotainment through newspapers and magazines. This cost-effective medium, however, is losing popularity to the Internet.
- Internet coverage embraces the Internet to provide information, news, views or entertainment online. This is one of the most popular and widely used forms of media today.

Having a centrally managed campaign would increase efficiency as the principle of economy of scale would apply.

Moreover, it would provide each Member State with ready-made material and content on which to draw as required and then 'localise' to suit the style and characteristics of their particular population/audience: this would remove any potential of offending users who may misconstrue certain aspects of a message. For example, if humorous content is provided in video format by one Member State, it may not be deemed acceptable or, indeed, funny in another Member State. Humour can be subjective and not everything works for all audiences. Additionally, posters may be provided and available for use but if a particular country has no mechanism for utilising this medium; it can be more selective on which material it uses and, conversely, provide alternative material that might work for other audiences.

Taking a European view means that the very best minds and experience from across the Union could be gathered together thus reducing the required investment from each stakeholder. This means that the level of return on investment (ROI) is increased and the focus can be placed on well-targeted, effective, communication(s) that can be used directly or tailored to local needs across the EU.



Leveraging on European and worldwide experience such as Insafe, which also runs annually in about 44 countries outside of Europe, and the StaySafeOnline.org campaign (<http://www.staysafeonline.org/>) would be an advantage.

### 4.1.3 Endorse and support

The Member States would have the choice to either endorse or support the European Month of Network and Information Security for All.

Endorsement is a way to officially show support and commitment for events — no financial contribution is required. In the case of European events organised to raise information security awareness, endorsers could include Member States, local governments and agencies. Benefits such as appearing on the official website of the European Month of Network and Information Security for All and in the media material, would be among the advantages that could be offered.

Alternatively, supporting would include several activities such as:

- sharing existing material
- contributing to the customisation of new and existing material
- implementation of the campaign
- dissemination
- financial help.



## 5. Engaging possible intermediaries

Awareness is not generally a priority spend for governments, computer emergency response teams (CERTs) or businesses. However, ignorance of risk through the lack of awareness is damaging core information security across the globe. Something clearly needs to be done. Why is this not the rallying phrase for increased spending? Because, despite what we try to demonstrate, the return on investment, especially with regard to the more secure behaviour of the private citizen, is very hard to prove in matrices and graphs and other things that look good.

Taking a European view means that the very best minds and experiences from across the Union could be gathered together thus reducing the required investment from each stakeholder. This means that the level of return on investment required to justify the spend is increased and focus can be placed on well-targeted, effective communication that can be used directly or tailored to local needs across the EU.

Intermediaries or third parties are people, organisations, or bodies who may get involved in the 'European security month' project before it moves on from the original producer to the final user.

### 5.1 Targeting intermediaries

The time and effort intermediaries can input is limited. Their time is, quite literally, money. Therefore, it has to be worth their time and effort: this can be achieved in a number of ways.

- Engage intermediaries for disciplined (in terms of time commitment) and meaningful (in terms of their being able to see their role) ways.
- Let the ultimate end product be clear from the beginning and delivered in a meaningful way.
- Treat the time and expertise of the stakeholders with the greatest respect so it is not wasted or forgotten.
- Communication is a two-way process and the stakeholders and intermediaries themselves are the best source of information as to their desires regarding outcome.
- Local variations in communication to citizens is acknowledged and respected.
- The time frame needs to be realistic, so the outcome can be delivered, and within a budget year, so any ROI can be noted: this may make it easier to raise interest and investment in the future.
- Identify the benefits the campaign will have for the intermediaries' constituents so they can see the value of the effort they will expend: this may require tailoring the message so that it highlights the benefits most suitable to each target audience.

A key enabler to the success of the campaign will be to engage with the most appropriate, influential and effective intermediaries. These intermediaries should be identified in the early stages of planning the campaign and selected according to how active and influential they are with their own constituents or with citizens.

These intermediaries can also be engaged at a number of levels to ensure a consistent message is communicated to the target audience.

- **European level:** If the intermediary body has a European representative body, then it should be brought on board to help create the most appropriate message for its members and constituents. It could also play a key role in identifying and engaging with the appropriate people and bodies at the regional, country and local levels. It is also important to remember that cybersecurity is an international concern and, therefore, engaging at the European level can assist in getting cross-border cooperation for the campaign.
- **Supranational level** <sup>(27)</sup>: Certain representative bodies may be represented at supranational levels, for example the Scandinavian or



<sup>(27)</sup> Here we refer to the regional level as a cross-border cooperation scheme.

the Benelux regions. Similar to engaging at the European level, engaging at the supranational level will ensure senior stakeholder support for the campaign and the ability to identify and interact with the appropriate people at other levels.

- **National level:** This is probably the most important level at which to gain intermediary buy-in. While support at the European and/or regional levels is a key success factor, it is the national intermediaries who are best positioned to engage with the ultimate end-users of the campaign. The role of a national intermediary will be to make sure that the key messages of the campaign are delivered: this may require the intermediary to tailor the message to factor in local and/or cultural nuances that may not be apparent to those outside the country.
- **Regional/Local level:** For larger nations, it may also be worthwhile engaging with intermediaries that represent local regions within their country. Again, this is to make certain that key messages are tailored for the local environment and culture.

Engaging with intermediaries at the appropriate levels will help to get the right people and organisations involved so that the campaign can reach as wide an audience as possible.

## 5.2 Intermediary types

Intermediaries come in various forms. They can be influential individuals, industry representative bodies, user groups or consumer representative bodies. Each intermediary will have their own audience that they will cater for and, therefore, each engagement will have to be tailored for each intermediary so they can see the benefit for their audience. While many of these intermediaries may not be involved in information security or information security awareness on an ongoing basis, they will no doubt be aware of the issues from sources such as the media or, indeed, the experiences and/or misadventures of their own audience.

There are a number of intermediary types that can be targeted as shown in Table 7.

**Table 7:** Types of intermediary

Intermediary type	Description
<b>Industry representative bodies</b>	These bodies represent the industries in which they are involved. These would include bodies that represent industries such as banking, finance and construction to name but a few. They often represent companies and organisations and would have an influence within their industry. Targeting specific intermediaries in this group such as bodies representing banks, the Irish Banking Federation, for example <sup>(28)</sup> , would help in getting their members engaged in the campaign.
<b>Government bodies and departments</b>	Engaging with government departments or bodies that are tasked with working with organisations, SMEs or the individual should also be used to help promote the campaign. Bodies such as consumer agencies, CERTs, regulators (especially those in the communications, financial or consumer spaces), agencies that support the development of small business, and industries and bodies charged with crime prevention would be excellent resources to employ in the campaign.
<b>Professional bodies</b>	These bodies represent the individual professional and would have the ability to either recruit individuals to disseminate the key messages of the campaign or to ensure the campaign message reaches their member base. One group that could be targeted would be the IT professional bodies, such as BCS <sup>(29)</sup> ; another profession that would have access to key target audiences, such as the SME sector, would be accounting. By engaging with their members, many of whom work in or for SMEs, the campaign message could be delivered to a key demographic. Representative bodies for the accounting profession in the United Kingdom are, for example, the Chartered Institute of Taxation <sup>(30)</sup> and the Institute of Chartered Accountants <sup>(31)</sup> .

<sup>(28)</sup> <http://www.ibf.ie> (last accessed 24 May 2011).

<sup>(29)</sup> <http://www.bcs.org> (last accessed 24 May 2011).

<sup>(30)</sup> <http://www.tax.org.uk> (last accessed 24 May 2011).

<sup>(31)</sup> <http://www.icaew.com> (last accessed 24 May 2011).

<b>Information security professional bodies</b>	Groups such as the Institute of Information Security Professionals <sup>(32)</sup> , Information Systems Security Association <sup>(33)</sup> , ISACA <sup>(34)</sup> , (ISC) <sup>2</sup> <sup>(35)</sup> and the SANS Institute <sup>(36)</sup> can be quite effective in getting information security professionals involved in making others aware of the campaign. In many cases, for members to maintain their membership status they have to gain points for Continual Professional Educational (CPE) on an annual basis. With the appropriate support from the representative body, it could be possible to encourage a large number of skilled and knowledgeable experts to become involved in the campaign, either in developing the content or delivering it to various audiences.
<b>Business networks</b>	There are a number of business networks which could act as very effective intermediaries by, in particular, reaching out to the SME sector. A prime example would be the Chambers of Commerce which would have a large number of members in the SME sector, for example the Irish Chambers of Commerce <sup>(37)</sup> . Many of these business networks are structured from the local, to the national, to the regional, the European and, indeed in some cases, the global level, thereby providing an excellent vehicle to reach all levels with the campaign message. Engaging with such business networks would help with the campaign and also assist the business networks to support their members to protect their key business assets.
<b>Celebrity involvement</b>	It can be difficult to reach out to citizens and engage them in a security awareness campaign. This is especially true when the campaign has to compete with many other campaigns such as those on road safety or health issues. Depending on the theme for the month of network and information security, it could be beneficial to engage with well-known individuals or celebrities to assist in spreading the message. Ideally, these individuals would be well known within their local or regional areas and be altruistic in giving their time to support the campaign. The individuals could be well-known sports people, radio hosts, TV hosts or musicians, for example.
<b>Social networks</b>	While social networks can be used to promote the campaign, it would also be worthwhile engaging with the social networking companies and getting them involved in the campaign. Many of these social networks struggle to promote a positive image with regard to security and privacy: getting involved in a campaign so that the message can be broadcast to their users would be of great benefit to not only the campaign, but also for these companies by promoting their image in protecting their users' interests. The social networks involved could be the major names such as Twitter and Facebook but should also include those social networks that target specific countries or languages, such as Tuenti <sup>(38)</sup> , which is a popular social network in Spain, Skyrock <sup>(39)</sup> , with its focus on French-speaking people, Friends Reunited <sup>(40)</sup> in the United Kingdom and Grono.net <sup>(41)</sup> in Poland, to name but a few.

<sup>(32)</sup> <http://www.instisp.org> (last accessed 24 May 2011).

<sup>(33)</sup> <http://www.issa.org> (last accessed 24 May 2011).

<sup>(34)</sup> <http://www.isaca.org> (last accessed 24 May 2011).

<sup>(35)</sup> <http://www.ics2.org> (last accessed 24 May 2011).

<sup>(36)</sup> <http://www.sans.org> (last accessed 24 May 2011).

<sup>(37)</sup> <http://www.chambers.ie> (last accessed 24 May 2011).

<sup>(38)</sup> <http://www.tuenti.com/?m=login> (last accessed 24 May 2011).

<sup>(39)</sup> <http://skyrock.com> (last accessed 24 May 2011).

<sup>(40)</sup> <http://www.friendsreunited.com> (last accessed 24 May 2011).

<sup>(41)</sup> <http://grono.net> (last accessed 24 May 2011).

## ENGAGING POSSIBLE INTERMEDIARIES

<b>Influential social media individuals</b>	There are a number of individuals who use social media to promote awareness of network and information security. By identifying and engaging key individuals who are actively blogging on such issues or are active on Twitter or Facebook, the campaign messages can be spread to an engaged audience who, in turn, will spread the message to their own followers.
<b>Media and press</b>	This is a very influential and powerful group that must be engaged successfully in order to ensure the campaign messages reach citizens in a manner they can relate to. In order to successfully engage with this group, it is important that the branding and key messages for the campaign are packaged in such a way to ensure their attention. It should also be remembered that the media need not be confined just to the national press and media outlets. Many of the intermediary types outlined earlier also have publications for their members and that is a medium that could be used with good effect to spread the messages from the campaign.
<b>Vendors</b>	One other group that can act as an excellent intermediary is vendors, particularly those in the IT and/or telecommunications sectors. They may be product vendors such as software and hardware companies or service providers such as telecommunication carriers, Internet Service Providers and/or hosting providers or large electronic retailers. By engaging with these organisations it may be possible to reach out to their clients. There may also be the opportunity to engage with some of these bodies to provide support in the form of financial contribution to cover the costs of the campaign.
<b>Academia</b>	Universities and research centres could act as very effective intermediaries by, in particular, reaching out to young people. Engaging with them, for example by featuring national/European cybersecurity competitions, would help with the campaign.

If Europe engages in joint activities with the United States, it would be key to exchange experience on awareness models and mechanisms, in particular on how best to involve intermediaries, for example telecommunications operators, ISPs, hardware, software and information services providers, in the delivery of messages to users about online behaviour and in the development and delivery of appropriate materials. Moreover, leveraging on the industry board members of the National Cyber Security Alliance (NCSA) would be an advantage. Most of the companies taking part in the NCSA have European headquarters which could be contacted to explore the possibility of extending their support to the European territory.

### 5.3 Endorsers and sponsors

The intermediaries would have the choice to either endorse or sponsor the European Month of Network and Information Security for All.

As mentioned earlier, endorsement is a way to officially show support and commitment for events — no financial contribution is required. In the case of European events organised to raise information security awareness, endorsers could include schools and universities, private companies, non-profit organisations, and community groups. Benefits such as appearing on the official website of the European Month of Network and Information Security for All and in the media material would be some of the advantages that could be offered.

The US National Cyber Security Awareness Month encourages all endorsers to partner the organisers on events and educate their employees, customers, suppliers, students, etc., and to sign an endorsement approval form which commits the endorsers to helping educate others about Internet safety and security. The endorsement approval form used by the StaySafeOnline.org is presented in Appendix III.

Sponsorship is similar to endorsement. The main difference is that it requires financial support. The balance between commercial support and funding and commercially agnostic campaigns should be considered.



Commercially agnostic campaigns (i.e. those with no visible sponsorship or company branding) can often be poorly funded, especially in financially difficult times where budgets are already stretched.

Alternatively, accepting sponsorship can create ethical difficulties, especially if more than one company for a specific sector or product isn't given the opportunity to 'tender' for sponsorship opportunities.

Sometimes, a company's motives for sponsorship are altruistic in order to create goodwill in the community, which increases their reputation. However, sponsorship is more commonly used to derive benefit from the associations created for a company's brand(s) or image as a result of the sponsorship.

An alternative area for support may be sector-specific organisations such as:

- banking organisations such as the European Banking Federation (EBF), the Irish Banking Federation (IBF), the British Bankers Association (BBA) and their European counterparts;
- payments bodies <sup>(42)</sup>;
- others with a vested interest (e.g. the Data Protection Commissioner, Information Commissioner, etc.).

Sector organisations such as the IBF are funded by commercial banks but may remove some requirements for multiple sponsorship and logos, etc. In Ireland, the IBF have contributed and provided support for previous campaigns held at national level in events such as the makeITsecure campaign (<http://www.makeitsecure.org/en/index.html>), held across the whole of Ireland (Northern Ireland and the Republic of Ireland).

In the United Kingdom, annual events such as Get Safe Online (<http://www.getsafeonline.org/>) have a mixture of private and public funding. The selection of sponsors for private funding in such events can, in itself, lead to problems, as commercial competitors may not be welcome or may compete to get higher 'billing' or visibility for their brand.

Organisers should consider support from security industry bodies — ISF, (ISC)<sup>2</sup>, ISACA, IISP, etc., or national standards bodies. (ISC)<sup>2</sup> runs a competition every year in which security professionals contribute security awareness material that is then made freely available for public awareness.

An example of this in action is the (ISC)<sup>2</sup> Cyber Exchange, which is a public awareness hub that houses information security awareness materials donated by the certified members. Anyone can download fun awareness posters, presentations, videos, etc. for free and share them with friends, colleagues or people in their community, to encourage them to protect themselves online.

Organisers should also consider support from non-commercial bodies such as universities and schools, IT associations and public sector bodies.

## 5.4 The message

It should be noted that in order to successfully engage with each intermediary, it is important to be aware that each one will require a message tailored specifically to them and their audience. A campaign message that is aimed at businesses will not work for an intermediary that is focused on the consumer; likewise, a consumer-focused message may not work well when delivered to a business. Therefore, during the development of the campaign, it is important that this is taken into account and that the campaign is customised for the intended intermediary type and their audience.

Each intermediary will also need to see the value proposition (or 'what is in it for me') of getting involved in the campaign. So, part of the message will also be to sell the campaign to the intermediary and highlight how addressing network and information security issues can benefit not only them, but their members, society and the economy as a whole. To this end, it is important to engage national radio and TV channels, to include storylines relating to the messages, and to develop a relationship with the national press and media, to run articles in different magazines and newspapers.

<sup>(42)</sup> For example, <http://www.mastercard.com>; <http://www.ukpayments.org.uk>; <http://www.paymentscouncil.org.uk>; <http://www.theukcardsassociation.org.uk>

## 6. Making a 'European security month' interesting

The main goal of the European Month of Network and Information Security for All will be to change the target group's secure behaviour in a long-lasting and positive way. This can be realised by generating awareness about NIS and modifying perception of risks associated for example with the 'safe' use of Internet, social networks and mobile devices in general. The main difficulty of making a 'European security month' interesting lies on the fact that people are not attracted by information security matters per se. To this end, any security events organised under the umbrella of this project should be able to attract the attention of the target audience in a way to develop some interest on the matter and generate awareness about information security risks and threats.

### 6.1 Length of the campaign

Following the analysis of many information security events held in different European countries, it is apparent that the length of the campaign is key for any organisation that would like to embark such a project.

A review of the 127 security events which have been analysed illustrates that the majority of these initiatives have been organised over more than one day.

The effective length of an initiative run at European level would be key to engage the right stakeholders, Member States (i.e. ministries, governmental agencies or other organisations), intermediaries and citizens. A single day is easier to sell to the general public, but also easily lost with all the other 'special days', such as World Health Day or a day set up to support a specific charity or, in some cases, discreetly or subtly advertise a product. A week would be manageable (Australia runs the National Cyber Security Awareness Week since 2008) but possibly more difficult to coordinate across the whole of Europe. Because of the particularities of the European territory, it is likely that a significant amount of effort would be required in order for this idea to deliver its full potential across Europe in one week only. Even if an entire month appears to be a long time to hold people's attention, it would give a lot of scope for sustained awareness and media opportunities at European level. Every Member State would have the opportunity to organise security events within a fairly long time frame. However, the length of the campaign (31 days) would not correspond to the number of events organised in every country (31 events): the increased duration would only provide the opportunity for a proportional increase in the total number of events organised across the whole of Europe. The overall effect would probably be to have awareness activities running continuously for a full month across Europe and, hopefully, gaining the constant attention of the media and the public. While the US National Cyber Security Awareness Campaign confirms that this could be a good practice to be followed, the potential difference with Europe should be considered. The United States has national media channels that can address the whole country contrary to the Member States. In Europe, national media channels only address Member States, and so they would be probably addressing different subsets of events at different times.

### 6.2 Security topics

Along with an emphasis on the general need for information security, there are many topics which could be addressed in the European Month of Network and Information Security for All.

For the aforesaid security awareness month to have a sounded and positive impact it is important taking into account the specific needs of the different contexts and audiences the security topics are applied to. This is especially true within the European Union, which comprises a diverse variety of countries where the security awareness levels, technology infrastructure and local laws/regulations might present some differences. In addition, the security topics should be prioritised according to its relevance to each particular context, audience and the risks being addressed.

Recent policy documents, studies and experiences describe a wide number of security topics that could be included within the European security awareness programme. The Digital Agenda for Europe of the European Commission suggests some action areas which should be taken into consideration, such as the protection of individuals' privacy and personal data; the support to reporting points for illegal content online (hotlines) and awareness campaigns on online safety for children run at national level etc. Furthermore, ISACA produced a list of topics which could be addressed in awareness campaigns. Although the list is not exhaustive and not all topics and areas might be relevant for national events targeting the general public, it could be considered as a good starting point when planning and designing the 'European security month'. The full



list is available in Appendix IV. The tips used during the last US National Cyber Security Awareness Month could also be used to define common topics together with those used by ENISA during its campaign to raise information security awareness across Europe. Table 8 reports some of the topics <sup>(43)</sup>.

**Table 8:** Some topics used during the last US NCSAM

Topic	What to address
<b>Backups</b>	Necessity and impact of loss, secure storage and transport
<b>E-mail use and security</b>	Appropriate use of e-mail, potential risks, etc.
<b>Home computers</b>	Appropriate use and protection; potential risks
<b>Internet use</b>	Appropriate use of the Internet; potential risks
<b>Passwords</b>	Password rules and tips for a strong password; potential risks
<b>Malicious software</b>	Identification of potential viruses, prevention; potential risks
<b>Social engineering/phishing</b>	Identification of social engineering/phishing; potential risks
<b>Internet safety and security</b>	
<b>Gaming</b>	
<b>Online shopping</b>	Identification of potential risks when shopping online
<b>New media</b>	Identification of misuse of Facebook, LinkedIn, Twitter, Hyves; potential risks
<b>New devices</b>	Appropriate use of smartphones, note/netbooks, tablets; potential risks
<b>New threats</b>	Espionage; identification of identity fraud
...	...

To complement the aforementioned security topics and in order to address the always changing threat landscape, it would be beneficial implementing collaborative efforts with additional trusted sources within the information security industry: CERTs/CSIRTs, SANS, NIST, the OWASP and the DatalossDB Open Foundation are some examples of entities that could provide valuable information about emerging threats that need to be addressed within the European Union. This information can certainly contribute at the time of defining the security topics, priorities and target audiences to be included within the European Month of Network and Information Security for All.

A combined effort between the public and private sector would provide a wider and more accurate view of the current threat landscape, leading to significant improvements in the constructive results of the information security awareness events subject to this document.

## 6.3 Communication concept

The European Month of Network and Information Security for All should be inspired by a 'strategic communication', and provide a conceptual umbrella that could enable the EU Member States to integrate their messaging efforts so as to increase the effectiveness of the campaign. In short, it should allow Member States to create and distribute communications that, while different in style and details, have a common nucleus and an inner coherence.

A few clear messages should be transferred to the audience, regarding fundamental security concepts in a way that stimulates people's interest and curiosity. Content presentation is a key point in keeping the interest on the campaign. Moreover, it should be considered that the attention of the audience is limited in time and could be easily lost. Whilst the overall campaign planning often involves communication professionals, and content selection, presentation and structure is often left to technical experts. This may be useful but may also have a negative impact on the campaign itself, when for example the language is full of technical jargon and acronyms. The audience won't understand, and will often be even annoyed. Technical communication is often more focused on correctness and completeness, rather than on simplicity, and being clear and concise.

An interesting European Month of Network and Information Security for All could be realised by using:

- analogies
- real examples
- simple and effective messages

<sup>(43)</sup> *Security awareness – Best practices to serve your enterprise*, ISACA, USA, 2005; see also NCSAM Tip Sheets (<http://www.staysafeonline.org/cybersecurity-awareness-month/ncsam-tip-sheets>) (last accessed 25 May 2011).

## MAKING A 'EUROPEAN SECURITY MONTH' INTERESTING

- a variety of delivery channels
- interaction
- memorable examples (e.g. use humour)
- personal examples (could it also happen to me?)
- unique as well as used messages and activities (curiosity v repetition).

### 6.4 Targeted messages

The message and the target group are tightly linked; each affects the other. A communication approach should be tailored to ensure topics are relevant to each individual, based on their interest and knowledge. The message could be focused on dealing with a class of risk, for example threats to privacy, or by focusing on a specific technology, for example mobile phones. An audience with little prior experience of information security is more likely to identify and understand a message that relates to how they use or interact with ICTs. For example: 'When using your mobile phone you need to consider the following ...' is more effective than a general message about protecting privacy. Key messages must be tailored for issues and concerns specific to the different target groups. Marketing and communication professionals may be involved in this phase.

#### 6.4.1 Vocabulary for the messages

Communication is crucial for any information security project. It is critical to ensure that the right vocabulary for the messages is used to realise an effective campaign. The main goal of a project such as the European Month of Network and Information Security for All should be to change the target group's secure behaviour in a positive way. Thus, as identified in some studies conducted by ENISA, it is preferable to accentuate the positive aspects by avoiding certain negative terminology as much as possible, as illustrated in Table 9.

**Table 9:** Positive vocabulary to use in messages

Vocabulary	
<i>Terms to use</i>	<i>Terms to avoid</i>
Protect	Prohibit
Access	Prevent
Benefit	Risk
Allow	Deny
Capability	Limitation
...	...

#### 6.4.2 Image for the messages

As well as for the terminology used, the images associated with the messages should be positive. There is no single image that is right for a specific message; however, some images should be avoided as they might transmit negative values.

**Table 10:** Terms to use and avoid in images

Images	
<i>Terms to use</i>	<i>Terms to avoid</i>
Keys	Locks
Shield	Weapons
Employee	Thief
...	...

### 6.5 Communication channels

The selection of appropriate communication channels is critical, and is often the key for making a campaign interesting and successful. Each target audience will have its preferred and most effective communication channels, depending on a number of factors (their age, cultural background, etc.).

For example, while videos published on the Internet are a way to reach a wide audience, some target groups may prefer a different channel. In an awareness raising initiative, target groups should be reached through the channels they already use for their valuable or interesting communications, including TV, magazines, and schools. As an example, it is common that marketing initiatives destined to consumers are carried on in supermarkets, where consumers already go and where they may be willing to spend some time. In the same way, SMEs usually participate in meetings and trade fairs, and are much less willing to spend their time on anything else. Citizens may be reached through television, because those less knowledgeable in the use of the Internet will not look for information on the Internet itself.

For the 'European security month' it would be good to consider the use of iPhone, Blackberry, Windows 7 and Android apps as well as other smartphones as communication channels for the purpose of mapping available prompt information and publicising the events to targeted interest groups. The apps would make the users' experience smoother, allowing them to find the information they need directly through their mobile while they are on the move.

## 6.5.1 Availability of information

Many campaigns invested relevant resources for activities in the planned time frame of the campaign (a week, a month, etc.), with no planned investments and activities for the subsequent time frame. As a consequence, shortly after the end of the campaign, information (e.g. links) started to get stale, domain names were lost and websites were closed. It must be considered that during the European Month of Network and Information Security for All, the audience may become interested in the subject, but many won't act immediately, e.g. won't look for additional information on the website, but just remember its name and plan to look for information afterwards. In many cases, some people will actually look for information only when events trigger their attention again (a computer virus, something in the news, etc.). Only at that point will they remember the campaign, and the interest will be high enough to look for detailed information. In some cases, it happened that at this point there was no more useful information available. The planning should allow for at least a maintenance phase after the end of the campaign.

## 6.6 Competitions

In the proposal of the new ENISA regulation, ENISA has been called upon to organise, in cooperation with the Member States, the European Month of Network and Information Security for All, featuring national/European cybersecurity competitions.

Information security tends to be quite esoteric and difficult to approach, so the idea to introduce competitions either at European or national level is something to be considered by Member States, at least for selected target groups.

Awareness raising campaigns on NIS security often provide competitions for children and youngsters solely, as demonstrated by the extensive experience of Insafe with the organisation of the annual international award for the most successful campaign of the year. Generally, the data gathered did not show a significant number of competitions organised for college and post-graduate students as well as for adults. Examples of the recent research conducted include the Cyber Security Challenge organised in UK. This competition is open to individuals and teams who have to go through a series of national online games and competitions that test their cyber security abilities <sup>(44)</sup>; the US Cyber Challenge (USCC) develops and conducts competitions that enable participants – including high school, college and post-graduate students – to develop their skills, gain access to advanced training and achieve recognition with scholarships, internships and jobs <sup>(45)</sup>.

It would be important to feature within the European Month of Network and Information Security for All such competitions to reflect the most common areas of focus in the field of cyber security and inspire anyone considering filling the ranks of cyber security professionals.

The involvement of organisations, either public or private, and academia would be essential. The support and involvement of public bodies and leading universities and research centres, such as the Cabinet Office and the Royal Holloway, University of London for the Cyber Security Challenge in the UK as well as the Department of Homeland Security for the USCC, could act together in a cooperative programme to provide their users with state of the art security awareness training and university

<sup>(44)</sup> <https://cybersecuritychallenge.org.uk/index.php> (last accessed 29 August 2011).

<sup>(45)</sup> <http://workforce.cisecurity.org/competitions-camps> (last accessed 29 August 2011).

## MAKING A 'EUROPEAN SECURITY MONTH' INTERESTING

courses, using their combined economic power to bring the cost down. The savings achieved during a recent cooperative buying programme run in the United States to support a national campaign to raise awareness on Internet security were in the region of 90 % over commercial pricing <sup>(46)</sup>. Moreover, these organisations could act as very effective intermediaries by, in particular, reaching out to young people. Engaging with a young and dynamic audience, for example by developing national/European cybersecurity competitions, could help with the campaign.

Finally, competitions usually have a portfolio of prizes to reward and seek to help winning candidates through educational opportunities and bursaries, internships and access to professional expertise, knowledge and networking opportunities. For example, the Cyber Security Challenge organised in the UK selects prizes to enable successful participants' ambitions and to fit with where they are in their career. Table 11 shows the prizes offered by the Cyber Security Challenge.

**Table 11:** Examples of prizes offered by the Cyber Security Challenge organised in the UK

Prize	Example
Bursaries for university courses	GBP 3 300 funding towards an MSc in Electronics and Security, Queen's University, Belfast
Places on cyber security training courses	Funded courses provided by SANS Institute; a two week placement on the Detica Academy and free places on Open University courses
Access to professional expertise and resources	Opportunities to use the CREST test rig
Memberships of professional bodies	Annual membership of the Institute of Information Security Professionals (IISP), the British Computer Society (BCS) and the Information Systems Security Association (ISSA)

<sup>(46)</sup> Over 160 organisations participated and these included State Governments of New Jersey, West Virginia, Montana and Ohio, as well as multiple agencies in New York, California and Oregon, more than 100 universities and many US city governments.



## 7. Creating an identity

A security programme should have a clear identity. The creation of an identity is necessary from a marketing point of view, meaning the security message needs to convince and attract people. An identity ensures that national security awareness events are clearly differentiated from other campaigns and set in the correct context. It also helps the target audiences recognise and better retain the messages sent through the security awareness campaigns. The creation of an identity is one of the key success factors for security awareness.

### 7.1 Branding

In many ways, altering the perception of security is a multifaceted public relations campaign and nothing is as valuable in such a campaign as a good brand. It is a way of creating an identity and establishing expectations as to the value of a product or service. Brands and the way that they are portrayed have become such a part of life in the 21st century that they are hardly noticed. Their invisibility adds to their power; if they are not consciously seen, it means that the message has become embedded in people's minds. Many companies have been successful in creating names that are instantly recognisable and trademarks that are a part of the popular culture not only in their own countries, but around the world. They have meaning, and they make a promise to the buyers of the products these companies make: woe to the company that fails to honour those promises <sup>(47)</sup>.

Creating a connection with citizens is key for the success of a project such as the European Month of Network and Information Security for All and a brand can embody qualities to which citizens will feel drawn.

This section is about what branding is, what the key elements of branding are, and the different techniques for managing it. The impact design can have on branding and how this can be used to create a strong positive impact for the European Month of Network and Information Security for All is also considered. References are made to the American and Australian experiences of running similar campaigns.

#### 7.1.1 What is branding?

At a visual level, a brand can be defined as a name, term, sign, symbol or design, or a combination of these, intended to identify the goods and services of one organisation or group of organisations and to differentiate them from others.

Although sometimes thought of only in terms of commercial companies, branding is used by charities, international organisations and even countries. All use aspects of branding to create strong identities and communicate their values.

For the 'European security month' campaign, an agreed set of brand values and messages would be created around which the brand would be built. This would then enable the brand to be presented consistently, both visually and in terms of discussions or interviews.

Any audiovisual output that such a campaign produces — for example, slogans, posters, booklets, videos, cartoons and graphics — should be durable and capable of being used with as wide a range of audiences as possible.

#### 7.1.2 Why does the European Month of Network and Information Security for All need branding?

Although all branding is about communicating a clear offer to customers or users, branding in the public sector is not necessarily concerned with maximum market stand-out. In this case, the aim might be to create clarity and enable access to important information. So branding and design may focus on signposting this information or communicating issues clearly in order to change people's behaviour.

Clarity can sometimes fall foul of the complex nature of public sector projects, which are often run by a network of stakeholder organisations or partners.

The development of the European Month of Network and Information Security for All's brand is an essential element for the success of the project. The branding process will help to:

<sup>(47)</sup> *Creating a culture of security*, ISACA, 2011.

- define the values of the campaign:
  - credibly: the campaign will be supported by more than one organisation and Member States — the message will be collective
  - establish confidence in the quality of information
  - ensure consistency — the same information and messages will be used across Europe
  - ensure that the campaign is relevant and practical — the citizen will feel that they can make a difference and that they are being given worthwhile information;
- deliver the message clearly;
- confirm the credibility of the project;
- connect the Member States emotionally;
- motivate the Member States;
- build the Member States' loyalty to a common goal;
- engage the intermediaries;
- encourage confidence in the quality of the project;
- establish recognisability which can be leveraged in years to come.

Successful branding is about promoting the strengths of a project. In this particular instance, the branding would give messages an instant context and provide a unifying theme for the variety of activities and media that every Member State would use to convey that message. Building a brand will communicate the 'European security month' messages to citizens more effectively so that they immediately associate the project with their requirements. An effective branding can elevate this project into something unique and promote its strengths.

Therefore, it makes sense to understand that branding is not about getting Member States to choose the European Month of Network and Information Security for All over other choices, but it is about getting them to see this project as the only one that provides a workable and Member State-friendly structure to organise a 'European security month'.

### 7.1.3 Other countries' experiences

A strong brand is invaluable (Table 11), as demonstrated by the experiences of Insafe with the Safer Internet Day, the US Department of Homeland and Security (DHS) with the 'Stop. Think. Connect.' campaign and the Australian Government with the 'Stay Smart Online' campaign. These campaigns have shown that it is important to spend time investing in researching, defining and building the brand.

The brand needs to address the sum total of these countries' experiences and perceptions, some of which can be influenced while others cannot. To succeed in branding, the needs and wants of each country should be understood and factored in to the branding and the wider campaign. This should be done by integrating the brand strategies through the Member States' bodies and companies at every point of public contact.



**STAY SMART ONLINE**

More than anything else, the Member States will be responsible for making the brand work. It will be their work that ensures that everyone believes in the campaign; it is essential that the campaign is perceived by them as being relevant and that it takes notice and responds to any suggestions they may make to improve the delivery of the brand messages.

The key to using any brand images is that it becomes immediately recognisable. Once a brand has been selected it should be used consistently and it must be durable. It is also essential to consider cultural, language, vocabulary and translation issues, as what works





in one country may be ridiculous when translated into another language. Producing a glossary of essential and common terms is recommended.

Leveraging on the international experience in this field would be key. For example, the Insafe logo was created by the Safer Internet Centres <sup>(48)</sup> which also chose the theme and slogans from a selection put forward by the internal Safer Internet Day (SID) working group. All countries were invited to translate the slogan and adapt it in order to respect their cultural and social needs. Moreover, the DHS has produced identity usage guidelines for the ‘Stop. Think. Connect.’ campaign. Seven main areas have been included.

**Table 12:** Characteristics of a strong brand

No	Area	Description
1	The signature	The signature is made up of different components. The ‘Stop. Think. Connect.’ signature is made up of two components: the logo and the name. The signature is the most important element of a brand system. It is important to apply the signature properly and consistently across all media to maintain a unified brand image.
2	Application	The acceptable applications of a signature should be confirmed: for example, logo and name, or just the logo. The relationship should never be adjusted or changed by, for example, inverting the order of appearance of the logo and name. Usually, the logo is aligned to the right hand side of the signature.
3	Minimum size	The signature should never be scaled down to a size where the name becomes illegible.
4	Clear space	Leave some white space around the signature so that it will always be legible and clear.
5	Signature colours	The colours of the signature should be specified, for example by using the Pantone number. These colours should be used in all communications to strengthen the overall brand.
6	Signature colour usage	The signature can be used in colour or a black and white version, depending on the need.
7	Incorrect usage	The correct and consistent usage of the brand will establish and maintain the strength of the brand. The signature and its components should not be altered or distorted. Thus, the correct proportions, arrangement of name and logo, colours and usage in shape should be ensured.

#### 7.1.4 Brand development recommendations

In order to ensure that the visual branding meets all of the necessary requirements, it is recommended that a professional branding company is appointed. Requirements should be gathered from all Member States and the European Commission.

Overall, the branding should be simple, work across states and cultures and be capable of being applied to different media. The particular characteristics of the European territory, the different cultures and the 23 official languages, would suggest, despite the successful US and Australian experiences, using a signature that works primarily in a visual medium, with, say, an extremely strong logo, rather than a range of potentially confusing slogans. The use of only the visual logo would avoid the translation of a name or slogans into different languages. The visual logo would need to be meaningful without knowing the name of the campaign, simple to reproduce and scale. The signature should be capable of working effectively in colours, two or four, or black and white. The use of a two-colour logo will make the signature appear simple and clear and the costs related to its use will be contained compared to a full-colour logo. Coca-Cola is a good example of how even a simple single colour logo (red on a white background or glass bottle) can be extremely successful.

Finally, it must be possible to include in any of the material produced for the ‘European security month’ the logo(s) of any other organisation, be they a ministry, governmental agency or private company, participating at the event. Campaign branding guidelines would need to be produced to ensure that the integrity of the branding is maintained when used in



<sup>(48)</sup> The national Safer Internet Centres are members of the Insafe network and they are appointed by the European Commission following a call for proposals launched every two years. The Insafe network counts 30 countries: 27 EU Member States, Iceland, Norway and Russia. Another 40 or so countries outside of the Insafe network have set up their own national Safer Internet Day Committee to run the campaign.

## CREATING AN IDENTITY

conjunction with other branding or visual identities. DHS, for example, has produced identity usage guidelines for the 'Stop. Think. Connect.' campaign.

The three stages of the brand life cycle that need to be considered are the introductory period, during which the brand is developed and introduced; the growth period; and, finally, the maturity period in which the brand either extends to other services/products or its image is constantly updated. Without careful brand management, the maturity period can lead to decline and result in the brand being withdrawn.

Creating a brand

Managing the brand

Extending the brand

## 8. Capturing feedback and adjusting campaign objectives

It is recommended that a combination of quantitative and qualitative information be captured when collecting data, by which to measure the performance of a 'European security month' initiative. However, the most useful and common types are quantitative based. These include amongst others a focus on metrics such as number of citizens targeted, number of security incidents in the last year compared with the previous year, and number of hits to the website.

The data should be continually captured across all countries (as measuring performance and monitoring the effectiveness of an initiative should be done during and after execution), and should ideally be caught through automated processes.

Methods to capture data include among others: questionnaires, website statistics, general observations, statistics from data centres, focus groups, data from call centres/hotlines, number of reports to IT support, press clippings, newsletters, press releases, number signed up to online services, and number of people trained.

The feedback captured when delivering the programme's communications should be reviewed with a view to how future communications might be improved and made more effective. This information should be combined with the results derived from the evaluation metrics. The programme's objectives need to be revisited in light of the effectiveness results. Reviewing the objectives allows for a serious assessment to take place.

The experience gained since the launch of the programme provides the knowledge and understanding to adjust the programme to make it more successful. The kind of adjustments required could involve each and every activity and task performed in the context of the programme. The key is to make adjustments while maintaining the focus on the programme objectives and goals.

## 9. A roadmap towards coordinated annual awareness efforts

This roadmap has been developed taking into consideration the findings of the ENISA research and considering the particularities of the European territory compared to other areas in the world as well as the inputs of the awareness raising workstream of the EU-US Working group on cybersecurity and cybercrime.

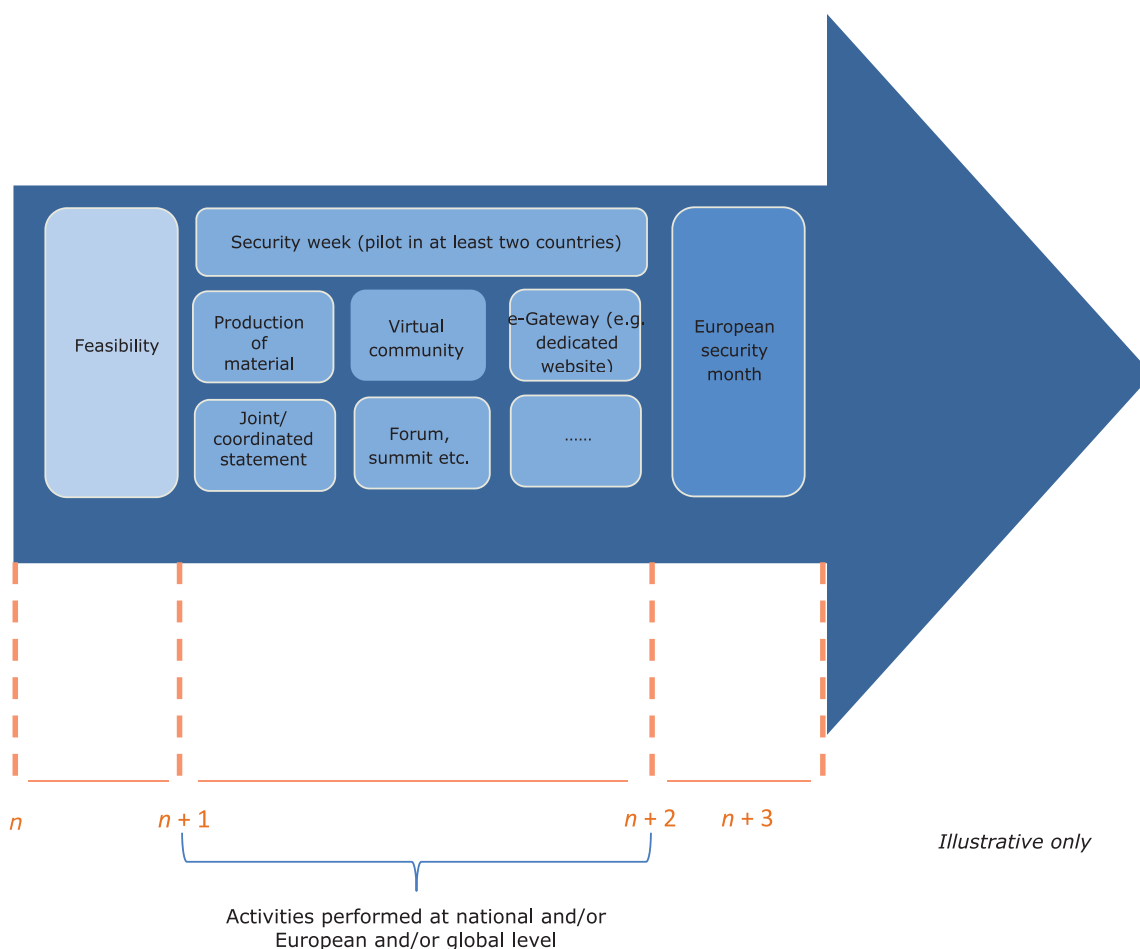
This element suggests that a significant amount of effort will be required in order that a 'European security month' delivers its full potential across Europe. To this effect, one of the most critical elements for the success of this activity would be to develop an effective structure and coordination scheme among participating entities.

Developing a roadmap has three major uses.

- It helps reach a consensus about a set of needs and the technologies required to satisfy those needs.
- It provides a mechanism to help forecast developments.
- It provides a framework to help plan and coordinate these developments.

This roadmap does not include any activity related to gaining/gathering political momentum or acknowledging the strategic opportunity of this project.

**Figure 4:** Roadmap of coordinated activities which will lead to the European Month of Network and Information Security for All



In this context, three phases have been identified. The first refers to the feasibility study that ENISA is producing with regard to the organisation of the European month of network and information security, in coordination with the activities of the EU-US Working group on cybersecurity and cybercrime. Materials and good practices should be collected in all EU

## A ROADMAP TOWARDS COORDINATED ANNUAL AWARENESS EFFORTS

countries in order to suggest coordinated activities. The second phase foresees various options of involvement and engagement at national, European and global level which will finally lead to the implementation of a 'European security month' (i.e. third phase). The third phase refers to the organisation of a 'European security month' in all EU countries. The month would define the boundaries during which each country would be required to organise one or more events to raise citizens' information security awareness.

Table 13 below describes some of the identified activities and lists the actors responsible for carrying out the initiative.

**Table 13:** Description of the suggested activities and related actors

Activities	Description	Actors			
		EC	ENISA	DHS	MSs
EU statement	The EU makes a joint/coordinated statement with the United States	✓		✓	
Member States' statement	The Member States make a joint/coordinated statement with the EU and the United States	✓		✓	✓
Global live webcast	The EU and the United States hold a live webcast	✓		✓	
Webpages	Create a set of webpages within the ENISA website, dedicated to the 'European security month'. Upload existing material and/or link back to other relevant documentation		✓		
Dedicated website	Create a dedicated website where material used across and outside Europe will be uploaded and/or link back. This website will be the gateway to successful European and international events and good practices		✓		
Material	The material to be used during forum/summit or events organised under the auspices of the 'European security month' will be produced and/or customised by ENISA, with the support of the Member States and eventually the United States. The material will follow the branding guidelines, for example with the inclusion of the 'European security month' logo. All material will be available in all 23 official languages and made available in a first phase on the ENISA webpages and then on a dedicated website. Relevant video clips will be also uploaded and shared through YouTube besides the ENISA webpages or a dedicated website. The use of apps will be considered		✓	✓	✓
Forum/summit and/or other events/activities	Organise an event in Brussels to inspire, enrol and give ownership to Member State(s)	✓			
	Organise events/activities across Europe under the auspices of the 'European security month' project				✓
	Issue and promote tips for better online security to Member State(s) on a daily basis for a week. This information security campaign will aim to engage Member State(s) and possibly intermediaries and partners. The messages will be promoted through activities online and events in different areas – metropolitan, regional, etc. – of the participating countries.		✓		
Pilot	Organise a security week in at least two Member States. As addressing the multicultural aspects is a critical factor, a pilot should include at least two countries with different cultures and languages. The Outreach and Awareness team will provide subject matter expertise guidance for participants of conferences, meetings and events				✓
Branding	Creating a connection with citizens is key for the success of a project such as the European Month of Network and Information Security for All and a brand can embody qualities to which citizens will feel drawn		✓		

When implementing any activity listed above, it is imperative that all roles are clearly defined. The RACI model<sup>(49)</sup> will be beneficial for doing so. Table 14 shows a sample of the RACI model with the activities down to the left-hand and, across the top, the roles of those responsible for carrying out the initiative or playing a part in it.

<sup>(49)</sup> RACI is an acronym for responsible, accountable, consulted and informed.



## A ROADMAP TOWARDS COORDINATED ANNUAL AWARENESS EFFORTS












**Table 14:** RACI model

Activities	Actors			
	EC	ENISA	DHS	MSs
EU statement	A R	I	I	I
Member States' statement	I	I	I	A R
Global live webcast	A R	I	A R	I
Webpages	I	A R	C	C
Dedicated website	I	A R	C	C
Material	I	A R	C	C
Forum/summit and/or other events/activities	A R	C	I	A R
	...	...	...	...
Pilot	I	C	I	A R
Branding	C	A R	C	C

A = accountable    C = consulted    I = informed    R = responsible

Member States might consider implementing or playing a part in one or more activities according to the level of engagement and information security awareness maturity of their country. As the level of effort, engagement and complexity of the identified activities varies, Table 15 suggests a different time frame for their implementation by using a scale of 1–3, the highest being 3. When an activity has been identified as recurrent, the full scale has been marked using a triangle (blue). Moreover, different colour codes have been used for identifying activities that could be eventually rescheduled based upon the type of effort, engagement and complexity involved as indicated in the legend below Table 15.

**Table 15:** Suggested time frames for implementing activities (using a scale of 1–3, the highest being 3)

Activities	Time frames ( $n + 1$ to $n + 3$ )		
	1	2	3
EU statement			
Member States' statement			
Global live webcast			
Webpages			
Dedicated website			
Material			
Forum/summit and/or other events/activities			
Pilot			
Branding			
....	...	...	...

Red = activity that cannot be rescheduled

Yellow = activity that can be rescheduled in the time frame +1

Pink = activity that can be rescheduled in the time frame  $\pm 1$

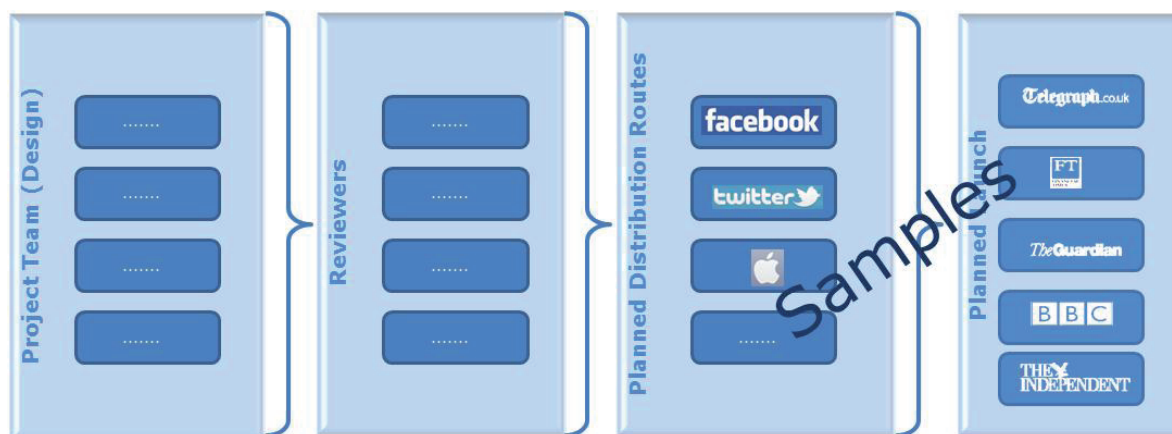
Purple = activity that can be rescheduled in time frame – 1

Green = activity that can be scheduled in the time frame 1-3 indifferently



Figure 5 shows an example of the structure required during phases 2-3. Social networks such as Facebook and Twitter as well as YouTube could also be used during this pilot as planned distribution routes. A media launch would be required. Advice, including the use of consistent messages, must be provided for Member States' bodies to share with national and local press agencies.

**Figure 5:** Structure required for phases 2-3



The analysis carried out by ENISA and the inputs of the awareness raising workstream of the EU-US Working group on cybersecurity and cybercrime appears to confirm that the method just presented in the roadmap description is the most complete and the one that meets the most requirements in relation to the organisation of a yearly 'European security month'.

## 9.1 Alternative methods to jump-start EU awareness activities

An alternative method to jump-start EU awareness activities is to design a minimal programme of events based on localities (some EU Member States, United States) where cybersecurity awareness activities have already been devised. The jump-start roadmap will select a minimum of two Member States as well as representatives of key communities (e.g. industry, academia) for a focused implementation of the first iteration of EU cybersecurity activities. To develop a programme which would engage the EU and the United States in joint activities, possibly starting with the coordination of events during 'a single week' and moving towards the coordination of yearly security months would be the ideal scenario. The experiences and lessons learned from these activities permit a rapid expansion the following year. The awareness months, in both privacy and security, were started in the United States in this way.

Another alternative would be for the jump-start to be effected by the European Commission, with the support of industry. For example, one option would be to create a forum/summit for the Member States to prepare joint activities the following year.

Leverage on the exchange of experts and material could be part of this activity. A possible delivery channel that could be used for helping raise citizens' awareness as part of this information security initiative is a shared website accessed by a virtual community. This would be the gateway to material such as video clips, posters, and leaflets. As shown by the data gathered by ENISA, websites are the most common delivery channel used by Member States that run either a security day or week across Europe. While the web content will be absolutely essential, it will be equally essential for other awareness raising activities to take place in order to ensure that the existence of the website is recognised and the content within it is used. Otherwise, a lot of good material will not actually reach the citizens who need it. Leveraging on existing good practices would be key for the success of such activity. This would lead to three main achievements:

- enhancing cooperation between Member States;
- reducing costs;
- keeping the pilot simple.

The implementation in coordination with the United States, where the cybersecurity month is established, is a supplemental model to jump-start the activities in Europe in the model where the first years are facilitated by the European Commission and ENISA.



## A ROADMAP TOWARDS COORDINATED ANNUAL AWARENESS EFFORTS

Concrete proposals in this direction can include the following.

- A public forum or debate on cybersecurity – potentially transatlantic –, with two or more physical locations, but broadcasted in a number of geographies via a webcast. Possible topics, potential participation, linkages with the US events could be defined as the forum or debate is planned. A community forum can be established as a result of such an event.
- A cybersecurity blog where public figures, representatives of private enterprises, experts and consumers discuss cybersecurity issues, with potential Q & A webcast sessions or Q & A areas of the blog. This approach will permit to socialising the ideas representing the focus of the cybersecurity event for a given year. The blog can be introduced at various events and conferences during the ‘European security month’ to increase its reach.
- An event dedicated to cybersecurity strategies developed in several Member States, possibly with the involvement of experts from the United States. Many Member States have released cybersecurity strategies in the recent past. These strategies share common goals, but also take somewhat different approaches to tackling cybersecurity issues. An event where these strategies can be presented and explained seems to fit well the introductory stage of the ‘European security month’.
- R & D events linked transatlantically – last October, for example, there was a substantial list of events in both Europe and the United States. Some of the events could have been linked in various ways, by sharing themes, scheduling webcasts, defining parallel sessions, setting up follow-up activities or communities.

The four proposed activities represent a sample of easy to organise and potentially linked events, with a substantial online presence that can form part of the first ‘European security month’.

## 10. Organisation modalities

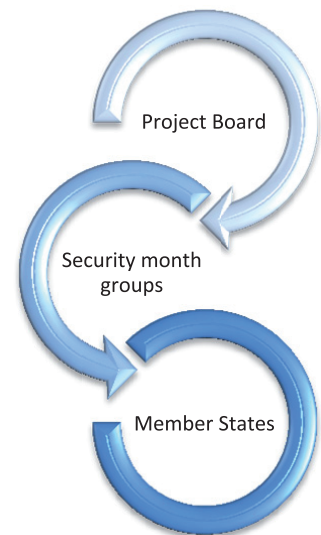
General project management notions would apply to the organisation of the European Month of Network and Information Security for All. Such project management activities would include the planning and allocation of financial, material, and human resources and the organisation of the work needed to complete the project across Europe <sup>(50)</sup>.

This section will not include the description of each project management process but will concentrate on the importance of the coordination role that, possibly, ENISA would play in such a project as well as that of the Member States.

There are a variety of organisation modalities that could be applied to this project. However, research carried out by ENISA reported that a decision-maker and someone to undertake the planning is essential, as well as national groups which should work to implement the 'European security month' activities at national level.

A Project Board should be established. Representatives of the European Commission and ENISA could potentially take part on this board, together with some experts of the EU-US Working group on cybersecurity and cybercrime and Member States. A similar structure is in place for the SID: the Safer Internet Day working group is composed of 10 Safer Internet Centres, Insafe and European Commission representatives. Centres are selected by applying the 'first in first served' principle. Usually, the same countries are not appointed for a second term if other candidates apply.

But, at national level, each group should comprise between one and a few organisations which work together with partners to implement the awareness activities. The 'Security month' groups will be supported by a team of people who will be the hub for all external engagement within the 'European security month' project. Moreover, they will provide subject-matter expert guidance for conferences, meetings and event participants. Data from Insafe and the DHS confirm this tendency when running projects of this nature.



### 10.1 Other countries' experiences

#### 10.1.1 Europe's experience

If we look at the organisations of the SID throughout Europe, three main actors are involved: the European Commission, Insafe and INHOPE. The level of effort and engagement varies from one organisation to another and it can be summarised as shown in Table 16:

**Table 16:** Effort expressed in number of man month(s) to organise the Safer Internet Day

Organisation	Number of man month(s)
European Commission	0.5-1 (depending on the type of event that is organised)
Insafe	9.5 (7 people for a total of 20 months within an overall 130 man months dedicated to the coordination of the network)
INHOPE	3

Different activities are performed before the SID and afterwards. From May until February – when the SID is taking place – all tasks involve the preparation and implementation of the SID. Every month at least two online meetings are held between Insafe and the Centres for approximately one hour to discuss the organisation of the day. From March until April, all tasks involve the assessment of the achievements and the production of the official report of the event. While all year long, one member of the Insafe coordination team dedicates one working day a week to work with the Centres on SID.

<sup>(50)</sup> *The new users' guide: How to raise information security awareness*, ENISA, 2010 (<http://www.enisa.europa.eu/act/ar/deliverables/2010/new-users-guide>) (last accessed 2 May 2011); PRINCE2 methodology (<http://www.prince2.com/what-is-prince2.asp>) (last accessed 2 May 2011).

## 10.1.1.1 Insafe's experience

In particular, the tasks and activities performed by Insafe are described in a dedicated work package that can be seen as a jump-start to EU awareness activity.

**Table 17:** Tasks of Insafe for organising the Safer Internet Day

	Tasks	Expected results/indicators	
		Qualitative indicator	Quantitative indicator
Insafe	<p><b>1. Organise an annual Safer Internet Day</b> (February) focusing on national and network-wide events and international reach, in particular on strengthening nodes' links with schools. Organise an annual international award for the most successful campaign of the year.</p> <p><b>2. Draft a detailed work schedule</b> for the event, working with a volunteer cluster of nodes during a 6-month lead-up, dedicating a network training session annually to ensure full participation and ensure prior consultation with the pan-EU youth panel. Describe in detail goals and expected outcomes, resources, dissemination strategies and time-frame.</p> <p><b>3. Liaise with the European Commission</b>, European and international Internet safety organisations and industry, building on past success to strengthen and deepen actions and maximise visibility and impact. Use leverage with education ministries for whole-school involvement. Liaise with SID committees in third countries at regular intervals throughout the year to make SID the central platform for ongoing cooperation.</p> <p><b>4. Implement an effective media coverage assessment procedure</b>, working with nodes and hotlines for a realistic view of impact/reach, defining relevant metrics and analysing areas for improvement.</p> <p><b>5. Publish media releases and an annual SID report</b> for optimal visibility across Europe and beyond, online and offline and at public meetings.</p> <p><b>6. Promote the Safer Internet Day campaign</b> and encourage hotlines worldwide to participate (INHOPE to lead).</p>	<p>1. National and international take-up of campaigns; dedication of SID committees in third countries</p> <p>2. Level of interest shown by media and industry</p>	<p>1. Level of participation by educational institutions and youths</p> <p>2. Number of events internationally and media coverage: minimum 1 000 media items per event</p>

A similar structure to that suggested for the Project Board of the European Month of Network and Information Security for All is the Safer Internet Day working group. This group is composed of 10 Centres and representatives of Insafe and the European Commission.

Safer Internet Day Committees are set up in third countries as follows: they must comprise one public and one private organisation. SID committees must promote and celebrate SID, and inform Insafe of how they celebrate the day; in return they can use the SID logo, press release and video. They are also invited to upload their profile and share resources at [www.SIDfair.org](http://www.SIDfair.org)

For what concerns the role of the private sector it should be said that the definition of the themes, messages or slogans is made without its involvement. The private sector is aware of the high visibility and impact of SID, and therefore seeks information and sponsorship opportunities from Insafe directly.

#### 10.1.1.2 US experience

If we look at the US experience, the outreach and awareness programme along with the State, Local, Tribal and Territorial (SLTT) engagement programme help support National Cyber Security Awareness Month, as well as general cybersecurity outreach activities. SLTT builds partnerships with non-federal public stakeholders including governors, mayors, state homeland security advisors, chief information officers (CIO) and chief information security officers (CISO), in an effort to advance the department's mission in protecting critical network systems.

The Outreach and Awareness (O & A) programme is the hub for all domestic external engagement within the National Cyber Security Division (NCSA). The O & A programme supports 'Stop. Think. Connect.' and National Cyber Security Awareness Month activities as well as providing subject matter expertise guidance to conferences, meetings and event participants. The O & A programme facilitates common messaging within the division as well as across the department. The organisational chart of the NCSA is presented in Appendix V.



## 11. Conclusions

The data gathered and the analysis carried out lead to the conclusion that organising a 'European security month' on an annual basis is feasible. The significant experience of some of the Member States in this field, and the commitment to achieve long-lasting change in human behaviour and perception of risks, are two essential elements that have been considered.

A European Month of Network and Information Security for All will be aimed to bring European countries together to raise awareness on NIS issues. Its organisation will bring benefits and advantages for the Member States. In particular it will:

- broaden the scope of national security events to make them a solely international event;
- improve image and positive public opinion about information security;
- reduce costs and, in this way, increase the efficiency of organisation of the individual security events;
- put leverage on ready-to-use material.

Equally, the 'European security month' will have benefits for the different target audiences. For example it will:

- reduce the number of incidents;
- increase the effectiveness and efficiency to detect, report and resolve incidents;
- increase the confidence of consumers/Internet users;
- protect children.

There are some important requirements to ensure success in the organisation of the European Month of Network and Information Security for All.

- The Member States must be engaged.
- All possible intermediaries should be involved.
- Consideration should be given to the support of sector-specific organisations, security industry bodies and non-commercial organisations.
- Media coverage must be used but avoiding negative messages or vocabulary.
- A brand should be built that improves the image and confidence in the project.
- A roadmap should be developed to plan and coordinate the project.
- A decision-maker and someone to undertake the planning is essential, as are national groups which work to implement the 'European security month' activities at national level.
- A Project Board should be established.

To conclude, ENISA believes this document will be a guide and support to the development and success of the organisation of the European Month of Network and Information Security for All.



## 12. Appendices

### 12.1 Appendix I – Inventory worksheet template

INFORMATION SECURITY AWARENESS WEEK/MONTH INVENTORY WORKSHEET				
Country name:			Security week? Y/N	
Programme name:				
Month(s):				
Organised by:				
Single point of contact (SPOC): (i.e. name of person in charge of the activity)				
Organised since	Last organised	Next delivery date	Frequency	Duration
Goals and objectives	Topic description	Target group(s)	Private sector involved? Y/N	
Delivery methods (brochure, comics, website, leaflet, clips, etc.)	Language	Type of messages used		
Link to website		Notes		

## 12.2 Appendix II – October 2010 NCSAM Proclamation

STATE/Territory of \_\_\_\_\_  
Office of the Governor  
State Capitol

**WHEREAS**, we recognize the vital role that technology has in our daily lives and in the future of our State and Nation, whereby today many citizens, schools, libraries, businesses and other organizations use the Internet for a variety of tasks, including keeping in contact with family and friends, managing personal finances, performing research, enhancing education and conducting business; and

**WHEREAS**, critical sectors are increasingly reliant on information systems to support financial services, energy, telecommunications, transportation, utilities, health care, and emergency response systems; and

**WHEREAS**, the use of the Internet at the primary and secondary school levels in this State enhances the education of youth by providing them access to online educational and research materials; and at institutions of higher education, the use of information technology is integral to teaching and learning, research, and outreach and service; and

**WHEREAS**, Internet users and our information infrastructure face an increasing threat of malicious cyber attack, loss of privacy from spyware and adware and significant financial and personal privacy losses due to identity theft and fraud; and

**WHEREAS**, the Multi-State Information Sharing and Analysis Center was established in January 2003 to provide a collaborative mechanism to help state, local, territorial and tribal governments enhance cyber security; and INSERT YOUR STATE/TERRITORY CYBER PROGRAM/OFFICE NAME provides a comprehensive approach to help enhance the security of this State/Territory; and

**WHEREAS**, maintaining the security of cyberspace is a shared responsibility in which each of us has a critical role, and awareness of computer security essentials will improve the security of NAME OF STATE/TERRITORY information infrastructure and economy; and


**WHEREAS**, the U.S. Department of Homeland Security ([www.us-cert.gov](http://www.us-cert.gov)), the Multi-State Information Sharing and Analysis Center ([www.msisac.org](http://www.msisac.org)), the National Cyber Security Alliance ([www.staysafeonline.org](http://www.staysafeonline.org)) and the National Association of State Chief Information Officers, ([www.nascio.org](http://www.nascio.org)) have declared October as National Cyber Security Awareness Month; and all citizens are encouraged to visit these sites, along with YOUR STATE/TERRITORY CYBER SECURITY AGENCY URL to learn about cyber security and put that knowledge into practice in their homes, schools, workplaces, and businesses.

**Now, therefore**, I, \_\_\_\_\_, Governor of the State/Territory of \_\_\_\_\_, do hereby proclaim the month of October 2010 as:

### Cyber Security Awareness Month

in the State/Territory of \_\_\_\_\_.

### 12.3 Appendix III – Endorsement Approval Form, National Cyber Security Awareness Month, October 2010



**StaySafeOnline.org**  
National Cyber Security Alliance

**National Cyber Security Awareness Month  
October 2010  
Endorsement Approval Form**

National Cyber Security Awareness Month (NCSAM), conducted every October since 2001, is a national public awareness campaign to encourage everyone to protect their computers and our nation's critical cyber infrastructure.

Endorsers of National Cyber Security Awareness Month recognize that individuals, organizations, business and government all share the responsibility to secure their part of cyber space and the networks they use. The steps we take may differ based on what we do online and our responsibilities. However, we all need to understand how individual actions have a collective impact on cyber security.

As an authorized representative of \_\_\_\_\_ (organization), I, \_\_\_\_\_ (name), hereby state that our organization agrees with the official Statement of Endorsement and endorses National Cyber Security Awareness Month. I acknowledge that the National Cyber Security Alliance and its partners may list our organization's name as an official endorser of National Cyber Security Awareness Month.

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Organization (as it should be listed by us): \_\_\_\_\_

Category: (check one)

☐ Industry ☐ Government ☐ Education ☐ Association/Non-Profit

We: ☐ will provide a logo (NCSA will contact you with technical specifications)

☐ will not provide a logo

URL to use in a link: \_\_\_\_\_

Contact Phone: \_\_\_\_\_

Contact Email: \_\_\_\_\_

☐ I wish to join the NCSA Mailing List.

**National Cyber Security Awareness Month 2010 Activities**

☐ YES, we will post the National Cyber Security Awareness Month Web banner.

☐ YES, we are holding an event for National Cyber Security Awareness Month.

☐ YES, please list the event on NCSA's calendar. Please submit information about your event online at [www.staysafeonline.org/content/events](http://www.staysafeonline.org/content/events). (You may also mail or fax your event information using the downloadable form found on the event submission page.)

☐ YES, we will share event metrics with NCSA.

**Please send this completed form to Joyce Perhac via email at [joyce@staysafeonline.org](mailto:joyce@staysafeonline.org) or fax at (412) 372-8136.**

**Note:** The Board of Directors of the National Cyber Security Alliance reserves the right to review organizations wishing to endorse.

Help us understand the reach of National Cybersecurity Awareness Month this is optional but we would like to know:

Your primary audience:

☐ Home User ☐ Business ☐ K-12 education

☐ Higher education ☐ Employees ☐ Customers

☐ Other (please specify) \_\_\_\_\_

Provide an estimate of the number of people you hope to reach: \_\_\_\_\_

What could NCSA provide that would make it easier for you to conduct awareness activities: \_\_\_\_\_

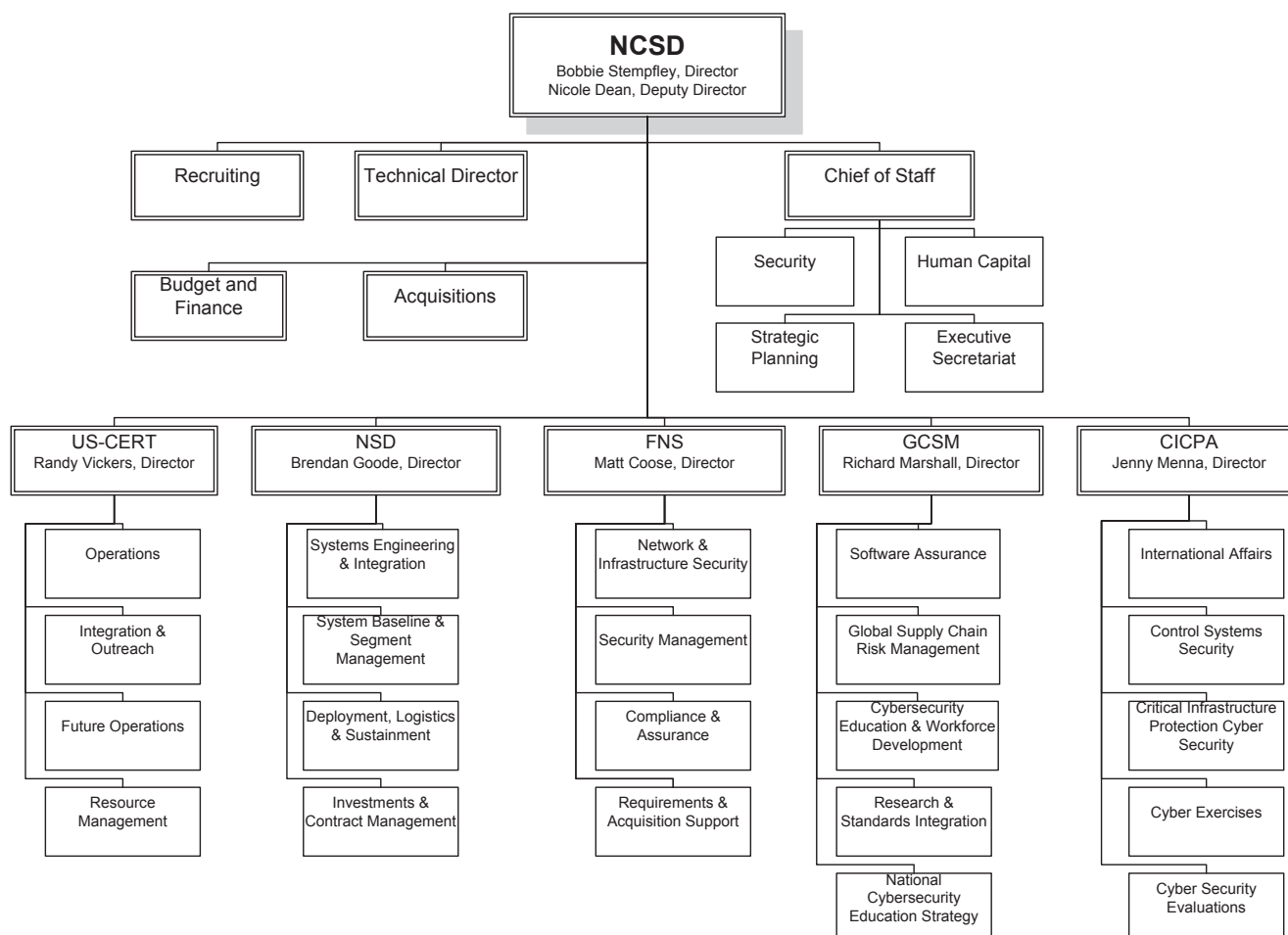
## 12.4 Appendix IV – Security awareness campaign topics

Example Topic	What to Address (potential issues and focus points)
Archiving	Labelling, secure storage and confidentiality
Backups	Necessity and impact of loss, labelling, secure storage and transport, and confidentiality
Badges	Personal use and visibility of badges
Clean desk	Clean desk policy
Data classification	Data classification levels, importance of confidentiality and labelling
Dial-up access to networks and computers	Use of authorised software and services only, security measures in place, identification and authentication for remote access
Disaster recovery	Recovery plan, recovery measures and responsibilities
Disgruntled or unhappy employees	Notification of management
Disposal of sensitive materials	Secure disposal, methods of disposal for different types of media
E-mail use and security	Appropriate use of e-mail, confidentiality of e-mail, potential risks, archiving of e-mails and encryption possibilities
Fax use and security	Appropriate use and confidentiality of fax
File-naming conventions	Conventions and standards for file naming in line with data classification
Fire/flood	Appropriate measures for fire and flood prevention and detection
Hackers	How to detect, notify and respond to suspicious network activities
Home computers	Use of corporate data on home computers, ability or prohibition of connecting to the corporate network
Incident reporting	How to report (security) incidents
Incidents	Overview of relevant incidents, especially those that occurred within the organisation
Information	Data that are considered to be necessary (that potentially need to be protected)
Information handling	Appropriate handling of information (in line with classification)
Information security	Definition and importance of information security for the organisation
Information security policy	Overview of the corporate security policy and a link to all relevant, related documents (standards, baselines, procedures, etc.)
Information security strategy	Elaboration on the corporate information security strategy
Instant messaging	Risks of instant messaging (viruses, Trojans, hackers, etc.) and appropriate use of instant messaging (if allowed)
Internet use	Appropriate use of the Internet (rules and guidelines) and the potential risks involved
Intruders and strangers	How to respond to unaccompanied strangers
Legislation	Relevant legislation such as privacy regulations
Media storage	Labelling, secure storage and transport, disposal, and confidentiality
Networks—WANs and LANs	Identification and authentication on the corporate network
Password changing, good passwords	Password rules and tips to make a good password that can be remembered, risks involved, prohibition to share passwords or to write them down, shoulder surfing

Example Topic	What to Address (potential issues and focus points)
PC use and security	Appropriate use of corporate IT equipment
PDA use and security	Appropriate use of PDAs and related risks (e.g. theft, loss, confidential information on less-protected devices)
Physical access	Physical access measures, use of badges, keys or biometric devices, holding doors, piggybacking, closing and locking doors
Portable computers use and security	Appropriate use of laptops, related risks (theft, loss, etc.). use of encryption and backups
Printouts	Confidentiality, storage and disposal
Repairs to equipment	Performed only by authorised personnel
Security of information: information systems when used offsite	General threats, vulnerabilities (risks) and appropriate safeguards of using information and information systems offsite
Smart cards	Use and storage of smart cards
Social engineering	Explanation on the definition and risks of social engineering
Software licensing	Licensing issues involved in the use of unauthorised software
Use of downloaded software	Prohibition of the use of unauthorised software
Use of personal software	Prohibition of the use of unauthorised software
Transport of sensitive information	Appropriate methods of secure transports for different types of media
Turning off/locking personal computers	Use of password-protected screen savers, locking or switching off computers when leaving them unattended
User programming	Guidelines (or prohibition) on user programming
Malicious software (viruses, Trojan horses, etc.)	Identification of potential virus or Trojan activity, prevention, virus scanner and notification
Visitors	Accompanying visitors, preregistering visitors, having visitors sign in and out



## 12.5 Appendix V – National Cyber Security Division (NCS) organisational chart



## 13. Index

### 13.1 List of figures

FIGURE 1	European overview	13
FIGURE 2	Languages used	17
FIGURE 3	Grouping of delivery channel(s)	18
FIGURE 4	Roadmap of coordinated activities which will lead to the European Month of network and Information for All	42
FIGURE 5	Structure required for phase 2-3	45

### 13.2 List of tables

TABLE 1	Categorisation of the target groups	15
TABLE 2	Security tips	16
TABLE 3	Cost estimations based on actual figures given from an airline corporation	21
TABLE 4	Performance indicators used across Europe	22
TABLE 5	Indicators used to assess the success of the NCSAM in the United States	23
TABLE 6	Benefits of the European Month of Network and Information Security for All	25
TABLE 7	Types of intermediary	28
TABLE 8	Some topics used during the last US NCSAM	33
TABLE 9	Positive vocabulary to use in messages	34
TABLE 10	Terms to use and avoid in images	34
TABLE 11	Examples of prizes offered by the Cyber Security Challenge organised in the UK	36
TABLE 12	Characteristics of a strong brand	39
TABLE 13	Description of the suggested activities and related actors	43
TABLE 14	RACI model	44
TABLE 15	Suggested time frames for implementing activities (using a scale of 1-3, the highest being 3)	44
TABLE 16	Effort expressed in number of man month(s) to organise the Safer Internet Day	47
TABLE 17	Tasks of Insafe for organising the Safer Internet Day	48

### 13.3 List of graphs

GRAPH 1	Month(s) when security event(s) are organised	16
GRAPH 2	Delivery channel(s)	20

European Network and Information Security Agency

**European Month of Network and Information Security for All – *A feasibility study***

Luxembourg: Publications Office of the European Union, 2011

ISBN 978-92-9204-056-7

doi: 10.2824/22578

Catalogue Number: TP-32-11-880-EN-N



P0 Box 1309 71001 Heraklion Greece  
Tel: +30 2810 391 280 Fax: +30 2810 391 410  
Email: [info@enisa.europa.eu](mailto:info@enisa.europa.eu)  
[www.enisa.europa.eu](http://www.enisa.europa.eu)



Publications Office

ISBN 978-92-9204-056-7

