European Cyber Security Month 2017

Deployment Report

FEBRUARY 2018

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use ecsm@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

ISBN 978-92-9204-246-2 DOI 10.2824/040879

Table of Contents

1. Executive Summary

For the fifth consecutive year, last October the European Cyber Security Month (ECSM) campaign was successfully executed across Europe. The campaign was coordinated and supported by ENISA, the European Commission, Europol's Cyber Crime Centre (EC3), European Banking Federation, the Estonian Information Systems Authority and cyber security organisations from the Member States. The support for which propelled the campaigns success as measured by both the qualitative and quantitative data compiled.

Although this year's campaign continues to break new records, the conclusions of this report highlight a number of fundamental areas that need to be addressed in the coming years if the campaign is to continue to grow and more importantly influence the security behaviour of citizens online.

Citizens across Europe face similar information security threats and information asset vulnerabilities; this is because most of the platforms, operating systems and devices used are produced by the incumbent global product/service providers. This applies to mobile phones, email messaging services, laptops and social media channels, since the vast majority of European citizens use similar technologies. However, citizens of each Member State have different levels of cyber security knowledge and behaviour. These differences across Member States may be triggered by the disparity of Member States in their commitment to awareness raising. In particular some Member States have a dedicated team of experts for planning and executing national security awareness campaigns; for example, the BSI in Germany and the ANSSI in France. Other Member States assign this role to a Ministry or Government CERT alongside their other core activities without a dedicated representative.

The effects of this is that there is a discrepancy between the measures that citizens may apply for the same or similar vulnerability or risk is one Member State compared to that of another Member State. An example of the situation, the Eurobarometer survey[1] highlights many differences across Member States in the use of cyber security measures, such as firewalls or the awareness of phishing attacks. Therefore, the different level of citizens' awareness and the potential risk-taking behaviour across Europe in turn leads to an increase in the risk level of Europe as a whole.

The concept for the European Cyber Security Month is to address this disparity across Member States in two stages. The first stage is to support the Member States so that the awareness and behaviour of citizens in each Member State is raised to a mature baseline. This becomes the reference baseline across the whole of Europe and thereby the European Cyber Security Month aligns the risk levels across Europe. The second stage is to further lower this risk by raising the maturity of citizen's behaviour in unison; at the European level. ENISA and the European Commission can achieve the objectives of the European Cyber Security Month by driving the pan-European campaign so as to ensure all Member States are actively committed to the European Cyber Security Month and that industry is also involved at all levels of the campaign both at the local and European level.

The ground work is in place for the European Cyber Security Month to move to the next level. This next level will be achieved only once a governance structure has been put in place as highlighted in the conclusions of this report. Furthermore a governance structure will ensure that the campaign is driven by MS as they are ultimately the benefactors of the campaign. A secondary reason for establishing a governance structure is

[1] [1] http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

to achieve another goal raised in the conclusions of this report which is to increase the commitment of the MS to the campaign and to bring on board those MS that have yet to designate a competent body to the campaign.

This report provides an overview of the activities organised and presents a synthesis of findings on the basis of evaluation and performance information gathered via a questionnaire and media monitoring data.

The report is structured into three main parts: an introduction, the implementation phase and an evaluation of the campaign.

The introduction will provide readers with the policy context, scope and target audience of the campaign.

The implementation phase of the report highlights the milestones that were achieved during the planning and execution phase of the campaign. This includes how events were organized and co-ordinated with partners, marketing materials used and insights into the execution of the campaign including results.

The final section of the report deals with the evaluation of the campaign, comparing this year's results with the previous year's and also provides input from the partners that was generated via a questionnaire; and finishes with a conclusion and outlook for the future.Documenting the activities of ECSM 2017 will assist in the organization and execution of future ECSM campaigns and allow for comparing the campaign with the results from previous years. The evaluation results and estimated impact of ECSM activities will provide the opportunity to discuss lessons learned deriving from this exercise and to helps draw attention to related concerns and opportunities for further improvement.

Finally the report is intended to provide a basis for discussion among the Member States, the European Commission and ENISA on how the ECSM can best be organised in the years to come. All Member States will need to face up to similar challenges, namely how to engage citizens and organizations so as to affect their information security behaviour.

2. Introduction

In 2013 the EU published the “Cybersecurity Strategy of the European Union”[2] as a means to safeguard the online environment and to provide the highest possible freedom and security, for the benefit of EU citizens. This strategy was jointly adopted by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy. It outlines the EU's vision in this domain, clarifies roles and responsibilities and proposes specific activities at EU level. Its goal is to ensure strong and effective protection and promotion of citizens' rights so as to make the EU's online environment the safest in the world.

End users play a crucial role in ensuring security of networks and information systems. In this context they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them. Several initiatives were developed in recent years. In particular, in October 2012, ENISA, with some Member States, piloted the "European Cyber Security Month" campaign.

In the context of the ECSM project, the Commission invited the Member States to organise a yearly cybersecurity month with the support of ENISA and the involvement of the private sector, with the goal to raise awareness among end users. ECSM and the private sector were also encouraged to join efforts in order to promote cybersecurity awareness at all levels, both in business practices and in the interface with customers.

ECSM runs for the entire month of October, with ENISA publishing new material and focusing on a different topic each week. Along with ENISA, various stakeholders, ranging from the private sector, academia, the European Commission (EC) and other EU bodies, joining together in a common vision by organising activities with special focus on training, conferences, online quizzes and provide general presentations to end users toward the establishment of an EU cyber-security culture.

This report summarises the activities carried out by ENISA and the participating MS for the 2017 campaign and presents the evaluation and conclusions of the campaign. More importantly, it seeks to trigger a discussion among partners with respect to improvements that can be made in the future.

2.1 Scope and Objectives

The scope of this report includes all the activities within the European Cyber Security Month (ECSM) campaign and their impact in 2017.

The main objectives of the campaigns within ECSM 2017 were as follows:

- to generate general awareness about Network and Information Security;
- to enhance awareness on information privacy and the General Data Protection Regulation;
- to promote safer use of the Internet for all users;
- to stimulate awareness on information security for Internet of Things;
- to build a strong track record to raise awareness through the ECSM;
- to involve relevant stakeholders and increase the participation of EU Member States;

[2] https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace

- to increase national media interest through the European and international dimension of the project;
- to enhance attention and interest with regard to information security through political and media coordination.

2.2 Evaluation Methodology

In 2017 ENISA developed an evaluation strategy to guide the Agency and MS with the gathering of data and information for the evaluation of the campaign. Member State coordinators were urged to consider and define the evaluation metrics duirng the planning stage of the campaign, so that the right data and information would be collected during the execution stage.

The evaluation strategy includes both quantitative and qualitative approaches from the following sources:

1. collection of quantitative data from the MS campaign coordinators,
2. feedback from the MS campaign coordinators via the end of year Q&A questionnaire, and
3. the use of media monitoring services to gather analytical data.

An evaluation data collection form (see Annex B) was developed by ENISA in collaboration with the Member State coordinators for the purpose of information gathering. The evaluation form aims at extracting pertinent information on the overall activities involved in the MS campaigns, their potential impact and includes participants' feedback. Guidelines (in Annex C) accompanied the data collection form, that highlight recommended metics for each type of activity

The evaluation strategy also included a questionnaite, where the aim was to extract information on the overall impact of the campaign based on MS campaign coordinators feedback with respect to ENISA's supportive role. Some of the elements assessed involve the level of support and its usefulness to MS, the impact of promotion material used and marketing strategies followed and the role of ECSM for improving the the outreach of MS campaigns.

The data gathered was procured by a media monitoring service and was aggregated by combining data elements from different sources to provide insights to identify the effectiveness of the messages, media channels and the campaign as a whole in reaching the general population.

2.3 Target Audience

This report is intended for organisations, either public or private, which supported the ECSM or intend to do so in the future. The report is also of interest to IT security professionals and other target groups who attended events and conferences organised across Europe during the month of October the past five years. Further, the report targets EU national policy makers who aim to improve the security awareness of citizens, professionals and generally IT end-users.

3. Planning Phase

3.1 The role of ENISA for ECSM 2017

3.1.1 Vision statement

ENISA's vision for ECSM is to support the Member States with the design and implementation of their awareness raising campaigns and to promote collaboration among EU Member States, international organizations and industry.

3.1.2 Mission statement

ENISA's mission for ECSM is to collaborate with the EU Member States and international organizations by finding innovative and fun ways to raise EU citizens awareness of cybersecurity, be they by organizing events, conferences, online quizzes, transferring of best practices or the use social media to educate and inform the public. Our mission is to enhance the delivery and synchronize ECSM among the EU Member States and industry that will share a pan-European vision and values for cybersecurity.

3.1.3 The Objectives for ECSM 2017

A consensus on the goals of ENISA for ECSM was reached with the participating MS. The goals that were recognized by all MS for the Agency are as follows:

- To promote the underlying value that is the foundation of ECSM:

"Cyber Security is a Shared Responsibility"

- To assist the Member States in implementing ECSM activities that satisfy certain criteria: have well-defined objectives, have well-specified target audience(s) per activity, have systematically defined cybersecurity subjects, have systematically chosen delivery channels and techniques and have well-defined effectiveness metrics
- To support the Member States in defining common areas of concern for cybersecurity that are shared and will be commonly promoted to EU citizens
- To support the Member States in delivering at least one cross-border awareness raising activity among at least three EU Member States
- To support the Member States with collaboration with the private sector

ENISA supported the organisation of the European Cyber Security Month campaign in various ways, such as:

- coordinator of the organisation of ECSM;
- hub for all participating MS;
- collector of available material and generator of synergies between MS;
- subject-matter expert on how to organise information security campaigns;
- subject-matter expert on how to design the content and evaluation strategy for information security campaigns;
- facilitator of common messaging within the participating MS by providing tips and advice on how to be safe and secure online;

- creator of the ECSM brand and related marketing plan;
- distributor of promotional material (posters and infographics).

The Agency coordinated the organisation of the ECSM campaign, by means of becoming a "hub" for all participating MS and providing suggestions, replying to enquiries and generating synergies between MS where possible. The Agency assisted the participating MS in defining evaluation methods and metrics during the planning phase, in order to ensure the alignment of campaign targets and evaluation approaches.

3.2 ENISA's Guidelines for Planning the ECSM Campaigns

ENISA developed and distributed a set of guidelines (see Annex D) to Member State coordinators for planning the ECSM campaigns from 2017 onwards. These guidelines related to three aspects of planning a campaign:

- **the objectives of security awareness,**
- **the development of a project plan to minimize unforeseen obstacles,**
- **and the formulation of a communication plan, including adequate delivery channels and content.**

3.2.1 A common Understanding of Security Awareness

Guideline 1: Member State Coordinators are encouraged to create campaigns aiming at activating users to protect information from security threats. Campaigns are expected to attract recipients' attention and make them recognize information security concerns and respond accordingly. ECSM campaigns should also strengthen users' abilities to accurately perceive potential privacy threats, with regards to their shared personal information.

3.2.2 Formulating a Project Plan

Guideline 2: Member State Coordinators are recommended to develop an ECSM project plan that can guide management with the design, execution and evaluation of the campaign. It is imperative to produce a documented project plan.

3.2.3 Creating a Communication Plan

Guideline 3: Member State Coordinators need to clearly define the target group or groups of the ECSM campaign. The Member State Coordinators can broadly separate target audience into general users, young people or business users. The design of the ECSM campaign should be customized upon the defined target groups.

Guideline 4: Member State Coordinators are encouraged to choose information security themes addressing both a) commonly identified security threats, and/or b) threats identified by national or international classifications as current security threats.

3.3 Coordination

3.3.1 Conference Calls and Meetings

ENISA maintained regular communication with the MS, in order to enhance collaboration and cooperation amongs the MS. The Agency scheduled monthly conference calls for the MS to share their plans for ECSM, receive and provide feedback and to support in the common promotion of the pan-European campaign strategy.

The Agency prepared and distributed the meeting agenda before each conference call. Meeting minutes where drawn up by ENISA after every call, and included a list of action points. The participation rate was high, with an average of 12 to 15 participates per meeting.

A physical meeting was organized by ENISA and held in Brussels in April 2017. The meeting gave MS the opportunity to discuss concerns and opportunities for improvements and finalize key areas of the campaign, such as the themes of the month, the collaboration infrastructure and the organization and logistics of the kick-off event.

3.3.2 Communication and Collaboration Technological Infrastracture

The collaboration mechanisms used for communication with MS is crucial for planning and executing the campaign. ENISA provided three types of software tools for maintaining communication:

1. file repository and file exchange tools,
2. teleconference software and
3. tools for the communication and collaboration between Member State coordinators and third parties (e.g., the private sector)

3.3.2.1 File repository and File Exchange Tools

ENISA proposed the utilisation of ENISA Sharepoint for accessing and storing files. The MS agreed on the necessity of a file repository and registered to the proposed platform. The file repository facilitated the work of the MS that was previously supported with the exchange of files via email.

3.3.2.2 Teleconference Software

Monthly conference calls were executed during the year in order to maintain regular contact with the MS. The selection of the teleconference software was noted as an important decision, given that there were a number of network and application restrictions on the side of the MS. In particular, certain tools (i.e., business versions, consumer versions) could not be utilised because they were restricted on the premises or the equipment of the coordinators' public agencies. The Agency acted as a facilitator by proposing several options and the coordinators gradually narrowed down the option to WebX which was used in the latter end of the year to host the monthly conference calls

3.3.2.3 Collaboration between Member State Coordinators

An important task during the planning of MS campaigns is the information sharing between the coordinators. Information sharing regarding the MS plans allows for the identification of synergies. In order to support the MS with this task, the Agency developed two templates to extract pertinent information.

- The Activities Template, is used by coordinators to document the awareness activities that are planned by the MS for ECSM. The ECSM activities template was designed by the Agency as a form with predetermined options (dropdown list) given the type of activity (e.g., workshop, TV advertisement, online activity), the relevant security theme and the target audience (e.g., home users).
- The Evaluation Template, is used by the coordinators to record the evaluation information for the executed awareness activities. The Agency prepared the evaluation report with predetermined security awareness metrics (e.g., number of advertisement impressions, number of conference participants) and the coordinators completed the adequate values.

3.3.3 Themes of the Month

ENISA organized a workshop on April 2017 in Brussels and invited the Member State coordinators to participate. The MS coordinators discussed and agreed upon the benefits of designing the MS campaigns around commonly agreed security and privacy themes. ENISA suggested during the workshop potential security themes and the MS discussed and debated on the most relevant and current topics based on MS cybersecurity priorities and the state of the art challenges. Following this discussion process, the MS gradually narrowed down the alternatives and determined four themes for the month, one theme for each one of the weeks in October.

The effectiviness of having themes of the month will need to be assessed to determine the optimum way to organize the themes during the campaign and / or whether focus should be placed on target audiences rather than threats / vulnerabilities.

The themes for 2017 were:

Week 1 - Theme: Cyber Security in Workplace

Targeting businesses, the aim of the theme was to raise awareness amongst employees and IT professionals about threats such as Ransomware, Phishing, Malware and provide general cyber "Hygiene" advice.

Week 2 - Theme: Governance, Privacy and Data Protection

GDPR countdown to compliance: Ensure you are ready!!! The aim of this theme was to uncover how to prepare your organization for the countdown to these new Directives and Regulations.

Week 3: - Theme: Cyber Security in the Home

The aim of the theme was to raise awareness amongst general users of threat from IoT, online fraud and how to protect their home network and protect their online privacy.

Week 4 - Theme: Skills in Cyber Security

The theme sought to support the young with gaining Cyber Security skills via training and education so as to grow the next generation of skilled Cyber Security professionals.

3.3.4 Press Releases

Member State coordinators distribute a formal press release before October announcing the ECSM and its activities. During the physical meeting in Brussels the Agency proposed that the coordinators collaborate so that the press releases could be distributed simuntaneously, to further foster a pan-European ECSM culture.

3.3.5 Kick-Off Event

Preparations for the fifth ECSM started in earnest with collaboration being forged between the Estonian Information Systems Authority, Tallinn University of Technology and ENISA for this year's Cyber Security Month kick-off event. The kick-off event was organized to take place during the EU Presidency in Estonia and the Digital Summit on the 29th September 2017.

An assessment of the goals and scope of the kick-off are needed if the event is going to be sustainable as a stand alone event without the financial support of ENISA. By determining the target audience of the kick-off event and the strategic objectives, a more effective event can be accomplished that will have greater outreach and publicity.

Private sectors involvement in the kick-off is currently limited to speakers / panellists for the sessions. A number of private companies approached ENISA during the year requesting to support the event by way of promotion and by sponsoring the lunch offered to the participants. Following discussions with the MS it was determined that further discussions were needed clarify the approach to take for involvement of the private sector at the European level.

3.4 Evaluation Strategy

3.4.1 Evaluation Objectives

The Agency aimed to ensure that all Member State coordinators would capture information during the execution of the awareness campaigns to enable the overall evaluation of ECSM and its impact. The objective of the evaluation was to assess the effectiveness of the awareness activities, the attractiveness of the activity, and its potential outreach and impact. The Agency urged the Member State Coordinators to determine the evaluation metrics they would be using at the planning stage to ensure that they collected the necessary data come the execution stage.

3.4.2 Evaluation Metrics

The Agency developed an evaluation strategy and a set of evaluation metrics for the Member State Coordinators to use. The evaluation metrics were incorporated into a template evaluation form, for each coordinator to complete upon finalisation of the execution stage. The evaluation metrics were segregated per activity type, given that different information is relevant depending on the type of awareness campaign.

3.5 Marketing Material

Both the Agency and the Member States were committed to raising awareness. A series of marketing channels and material were used to achieve this purpose, as presented below.

3.5.1 Visual identity

The Agency created some years ago a visual identity for European Cyber Security Month including a logo[3], a colour chart, typography rules, guidelines on use of imagery, design templates and a manual of formal guidelines on the proper use of these elements. ENISA updated the ECSM logo, in order to signify the 5th year anniversary for ECSM. The update logo for the 5th year anniversary is presented below:

[3] https://cybersecuritymonth.eu/press-campaign-toolbox/visual-identity

Figure 1: Updated logo for the ECSM 5th year anniversary.

The updated logo was used by ENISA, the Member States and all partners on their websites, material, videos and social media to link their efforts up to the European campaign.

MS showed keenness to adopt the 5 year logo in their local campaigns. The historical background of the campaign was now available and visible in the logo and as such added weight to the MS campaigns.

3.5.2 Slogan

The slogan "Cyber security is a shared responsibility!" remained unchanged in 2017.

3.5.3 Press releases

The Agency coordinated this year's Press Release[4] with the European Commission, to ensure maximum outreach and to stimulate attention to the featured activities and events. The Press Release was translated into all official languages of the European Union and was released on 2nd October instead of 29th September as in previous years so as not to be superseded by Digital Summit that was taking place on the same day in the same city as the kick off event. The services of a media company were procured to further disiminate the press release to national and region journalists and press across Europe.

3.5.4 Social media - banners

The Web and Social Media banners remained the same as in the previous years.

The banner was available in four formats to match different needs (i.e., 815x315, 1500x500, 1200x717, 1200x630).

Figure 2: ECSM 2017 social media banner.

3.5.5 Poster and Infographics

During the physical meeting in April in Brussels the MS discussed the different marketing options and their impact. As a result of this discussion the MS decided not to produce posters for this year, but instead to

[4] https://www.enisa.europa.eu/news/enisa-news/european-cyber-security-month-united-against-cyber-security-threats

allocate the relevant resources for the production of more videos, because of their perceived higher impact and reach.

3.5.6 Videos

Four videos where produced for this year's campaign, one for each themes of the month. Each of the videos were designed to be less than 1.30 minutes long and they were shot without narration so that the message would be conveyed via picture and text displayed at intervals, which could be translated by the MS if required.
The first video5 for theme 1 (Cyber Security in Workplace) was a video promoting good practices for cyber security protection in the workplace.

The second video6 for theme 2 (Governance, Privacy and Data Protection) encouraged organizations to consider the implications of the new regulation and legislation on personal data protection.

The third video7 for theme 3 (Cyber Security in the Home) demonstrated the implications of security for the Internet of Things and smart technologies in the home so as to encouragecitizens to be aware of these cyber security threats.

The fourth video8 for theme 4 (Skills in Cyber Security) aimed at raising awareness of the career opportunities in Cyber Security.

3.5.7 Website

The material on the ECSM website[9] was re-organized including the tabs on the home page so as to enhance the accessibility of the website. .

[5] https://www.youtube.com/watch?v=KM67LrJ18VE
[6] https://www.youtube.com/watch?v=5EG8zRrC_6s
[7] https://www.youtube.com/watch?v=CR51XZjLvRs
[8] https://www.youtube.com/watch?v=0pN6a20Kf5Q&feature=youtu.be
[9] https://cybersecuritymonth.eu/

Figure 3: Map of ECSM 2017 activities across Europe

3.5.8 NIS Quiz

The NIS Quiz remained the same for ECSM 2017. Is was decided at the ECSM meeting in April that the NIS Quiz would not be enhanced in favour for other activities.

3.6 MS Campaign Coordinators

The following table is a list of national campaign coordinators for ECSM 2017:

Organization	Member State	Organization	Member State
Estonian Information System Authority (CERT-EE)	Estonia	Executive Agency for Electronic Communications Networks and Information Systems (ESMIS)	Bulgaria
Ministry of Digital Policy Telecommunications and Media	Greece	Research and Academic Computer Network in Poland (NASK)	Poland
Centro Nacional de Cibersegurança (CNCS)	Portugal	Communications Regulatory Authority (RRT)	Lithuania
Latvijas Republikas Aizsardzības ministrija (MoD Latvia)	Latvia	Federal Chancellery of Austria (BKA Austria)	Austria
Ministère de l'Économie Direction du commerce électronique et de la sécurité de l'information (CASES)	Luxembourg	Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)	Romania
Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)	France	Liechtenstein	Liechtenstein
SWITCH	Switzerland	Centre for Cyber Security Belgium (CCB)	Belgium
Finnish communications regulatory authority (FICORA)	Finland	National Cyber Security Center (NCSC)	Hungary
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Germany	Departamento de Seguridad Nacional (DSN)	Spain
Norsk Senter for Informasjonssikring (NorSiS)	Norway	UK HomeOffice (GOV.UK)	UK
Ministerie van Veiligheid en Justitie (VenJ)	Netherlands	Critical Infrastructure Protection unit (Malta CIP)	Malta
Slovenian National Computer Emergency Response Team (CERT-SI)	Slovenia		

Table 1: List of ECSM campaign coordinators for 2017

4. Execution phase

4.1 Kick-off event

The kick-off event for the 5th ECSM was held under the Estonian Presidency at Tallinn University of Technology on 29th September 2017. The event was co-organized by ENISA and the Estonian Information Systems Authority. The agenda[10] included welcome speaches by the Director of the Estonian Information System Authority (RIA), the Executive Director of ENISA and the Director of DGIT at the European Commission. Moreover, it included speeches experts from from the European public sector and industry.

In dedicated panel sessions the ECSM national co-ordination teams offerred insights into their campaigns and leading IT security experts debated on the security themes of 2017.

The panel discussions centred around the themes of the month and the role of awareness raising within each of the topics. The group of panellists included esteemed cybersecurity experts from ADP, APWG, BHC Laboratory, CERT Estonia, CERT Latvia, CISCO, European Banking Federation, Europol's EC3, Hytrust, Intel, Tallinn University of Technology, and University of Erlangen-Nuremberg.

The event attracted over 90 participants and was also live streamed via the Tallinn University of Technology Youtube channel.

4.1.1 Week 1: October 2-6

Theme: Cyber Security in the Workplace

Targeting businesses, the aim of the theme was to raise awareness amongst company employees, IT professionals & senior management about threats such as Ransomware, Phishing, Malware and to provide general cyber "Hygiene" advice.

4.1.2 Week 2: October 9-13

Theme: Governance, Privacy & Data Protection

Countdown to compliance: Ensure you're ready!!! The aim of this theme was to uncover how to prepare your organization for the new EU Directives and Regulations such as the NIS Directive and the GDPR.

4.1.3 Week 3: October 16-20

Theme: Cyber Security in the Home

The aim of the theme was to raise awareness amongst general users of threats from IoT, online fraud / scams and provide guidance on how protect their home network and protect their online privacy.

4.1.4 Week 4: Oct. 23-27

Theme: Skills in Cyber Security

The theme sought to support the young with gaining Cyber Security skills via training and education so as to grow the next generation of skilled Cyber Security professionals.

[10] https://cybersecuritymonth.eu/draft-agenda/view

Week 4 also coincided with the launch of the European Cyber Security Challenge that was organised by the Spanish National Cybersecurity Institute INCIBE with direct involvement and support from ENISA.

The challenge, expert talks and job fair attracted a lot of interest, including over 200 of the best Cybersecurity talents and hundreds of visitors from across Europe, who came to network and to compete for the European crown.

Young talents from 15 competing national teams proved their technical and teamwork skills in the most exciting and complex cyber competition of the year. The jury had a tough task to select only one winning team, considering the very close final results and the intense competition on the day of the challenge.

4.2 Member State Campaigns

The following section provides insight into some of the Member States campaigns that were organized by ECSM coordinators.

The MS listed below are a selection of those MS that are active partipants in the organization of the ECSM campaign both at the European level and the local level. Ideally all MS will be actively involved in shaping the campaign in the future, which is why it is imperative that the campaign demonstrates to other MS the benefits and value of working together in such an endeavour.

4.2.1 France

The 5th edition of ECSM campaign was coordinated at the national level by ANSSI, the national authority for cybersecurity and cyberdefence, in France. The program of the campaign was ambitious, aiming to raise awareness and provide advice and recommendations in both the work place and at home. For the 2017 edition more than 30 French institutional actors and stakeholders (ministers, national authorities, associations), including political figures, were involved in promoting the ECSM initiative and useful advice both for their own employees and the larger audiences (private companies, general public, students, etc.). ANSSI also provided an awareness kit on the event to be shared widely, both in French and English with an official poster, web banners and mail signature with the colors of ECSM. Finally, a press conference took place on October, 2nd to present the national program.

Altogether, more than 70 activities were organized all over France (conferences, workshop, and exhibitions) registered on the ENISA official website as well as on a dedicated web page: (www.ssi.gouv.fr/mois-europeen/). Furthermore, a successful digital campaign took place all through October on Twitter and Facebook around a common identity (#TousSecNum and #ECSM) and the European themes. Three videos were produced by different institutions around the good practices, the ransomware threats as well as the role of cyberdiplomacy.

In numbers :

- 172 million messages viewed on Twitter and 14800 users actively engaged in the campaign in October
- 33500 tweets and retweets around #TousSecNum #ECSM
- 16600 views of the dedicated webpage in French (https://www.ssi.gouv.fr/agence/cybersecurite/mois-de-la-cybersecurite-2017/)

- 6114 download of the press release presenting the ECSM and more than 50 press articles published during the month

4.2.2 Germany

In Germany the Federal Office for Information Security (BSI) as the national cyber security authority shapes information security in digitization through prevention, detection and reaction for government, business and society. Thus, supporting the annual ECSM-campaign goes hand in hand with the efforts to raise awareness for cyber security among these diverse target groups.

In 2017 BSI won more than 100 partners in Germany who established more than 200 activities around October. The range of activities was quite broad, from webinars and social media activities to live-hacking events and a whole thematic day with workshops, discussions and many more. Overall, BSI succeeded in substantially bringing forward the ECSM campaign in Germany with a significant rise in partners and a higher outreach to citizens than in previous years.

As the national coordinator in Germany, the BSI supported the ECSM especially with activities focussing on private users. BSI adapted the weekly topics of ENISA and provided information material on each topic. Basically, these were:

- - four video-statements, each giving background information regarding the weekly topics,
- - four polls on Facebook, presenting questions on the weekly topics to interested users, and
- - press releases on each topic.

Furthermore, BSI focused on the topic "cybersecurity at home" for the whole month. In addition to the above mentioned activities, BSI published the following:

- - a new brochure for private users on the secure use of IoT- and smart home devices,
- - two website articles on how to secure smart homes,
- - an animated video informing about relevant security measures for smart homes,
- - a short quiz on the website to test user's knowledge on cybersecurity for smart homes, and
- - a radio feature on this topic.

Additionally, BSI supported an "action day" taking place in Bonn with a presentation and an information booth to give advice to interested citizens.

As coordinator of the ECSM and as the national cybersecurity authority the BSI will also be highly engaged in contributing to and promoting the ECSM in the coming years with even more ambition.

4.2.3 Luxembourg

The kick-off for ECSM 2017 took place on the Oct 12th during the opening of the Luxembourg Cybersecurity competence center by Francine Closener, Secretary of State of the Economy. The inauguration was followed by a dedicated Cybersecurity week Luxembourg, taking place from 16-21 November.

The *Cybersecurity competence center* is based on a public private partnership and part of SECURITYMADEIN.LU innovative services to provide users with up-to-date threat analysis, solution testing and immersive cybersecurity training through a dedicated simulation platform.

Cybersecurity week Luxembourg was filled with 15 events to support the build up of a culture of cybersecurity among individuals and to position the country as a leading European location for cybersecurity start-ups, talent, investors and experts who are looking for growth opportunities.

Founding members (Excellium, Luxinnovation, Ministry of the Economy, PwC; SECURITYMADEIN.LU) and supporters (Digital Skills coalition Luxembourg; Luxembourg Institute for Digital Training) of the Cybersecurity week Luxembourg brought together over 2000 people to participate in a variety of ICT activities. Public and private actors demonstrated their determination to collaborate towards improving the level of digital security of companies, organizations and citizens. On the international scene, Luxembourg has increased its visibility by attracting world-renowned experts.

PwC's Cybersecurity Day brought together more than 200 professionals, experts, public and private actors, start-ups and investors involved in international IT security issues as well as the tools and solutions of tomorrow thanks to 10 companies selected for their innovative solutions originating from Europe, the USA and Israel. The analysis of threats and vulnerabilities as well as the means to combat them, aroused the interest of all professionals looking for new ways to enhance their security.

"Hackers" from around the world gathered at the Hack.lu conference and set a new record: no less than 60 speakers took turns presenting their topics!

This spotlight on cybersecurity comes at the right time, when Europe is sorely lacking in professional IT profiles which will ensure the cyber defense of tomorrow. Creating professional career paths has become vital and the "Cyber Talent Day" event contributed to this goal.

On the regulatory side, the implementation of the GDPR in 2018 worries small businesses that do not always know where to start when it comes to compliance issues. The topic was discussed several times during the week, and helped to clarify things for these actors.

Other events included for example a "Cybersecurity4success" conference at the Luxembourg Chamber of Crafts; a "Hack4kids" and a "Crypto party" for kids gathering around 150 kids.

The week ended with the presentation of 5 awards: Best Security Officer (CISO); Best Thesis Award; Capture the Flag Award; Most Promising Company Award; People's Choice Award.

In addition, ECSM Luxembourg traditional partnership with BEE SECURE[11], a governmental initiative raising awareness among young people and public at large, was also successful this year: the ECSM is part of the BEE SECURE campaign "Big Data", gathering 18 national partners and associations and raising awareness about the "traces" we leave on the internet, and how to lead a responsible online life. The campaign is mainly displayed in schools and public spaces from October 2017 to September 2018. ECSM was also mentioned in their launching press release.

Furthermore, RESTENA, a foundation providing network services for all public and private institutions and organizations involved in the field of education and research, and the University of Luxembourg initiated a blog for their students and employees to raise awareness on cyber themes during ECSM.

A first, fruitful, contact was made with the European Investment Bank. We look forward to extend our cooperation for 2018 edition.

During the ECSM we promoted, among others, the 4 thematic video clips produced for the campaign through our social media channels. Generally speaking, press coverage was done through 3 press communiqués ; 8 articles in the national press; 1 radio show; a dedicated website with12,000 visitors during ECSM; approx.

[11] https://www.bee-secure.lu/

2500 Facebook followers and an organic reach of nearly 4000 people for #ECSM related post and 1200 tweeter followers.

4.2.4 Slovenia

For the 2017 European Cyber Security Month Campaign Slovenia focused on workplace security and cyber security challenges that small and medium companies are facing. The main creative idea that reflected in design, copy right and all communication channels (Facebook, TV ads, new website, online advertising) was that the mouse could be the most frightening animal as one wrong mouse click could cause big trouble in a sense of online security. During entire month of October, a new website targeting business users, more specifically accountants, employees and employers was established. The site focused on this target group and providedadvice so website users could find useful and tailored resources regarding ransomware, online scams targeting companies, malware, phishing, safe online banking, backup, GDPR, network security etc.

The website content hub included three main call-to-actions:

- Order a poster for your company. During the entire month of October, free posters were provided about ransomware for companies who expressed their interest.
- Sign up for newsletter. New mailing list for business users was set up and every Monday morning one tip about workplace security was distributed.
- Download Security Roadmap for your company. A booklet was published with 10 crucial information and network security challenges for SMB.

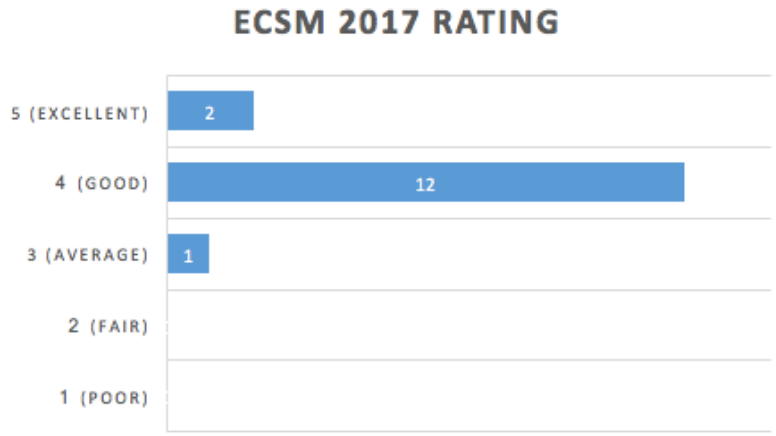
5. Evaluation

5.1 Questionnaire

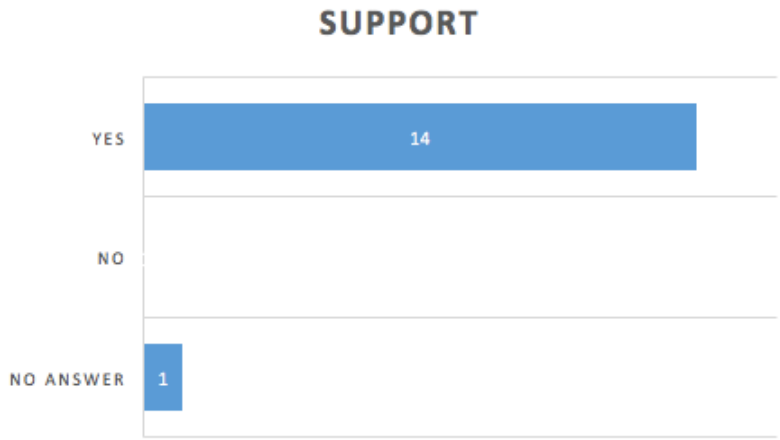
The questionnaire is an important tool used to gather the opinions of the MS coordinators that are engaged in the campaign. The charts below present the replies of 15 participants representing their MS. An increase of 3 participants compared to the previous year.

5.1.1 Results

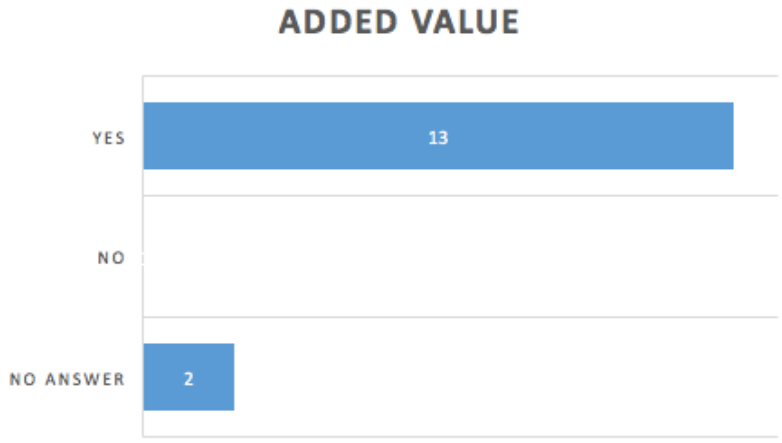
1. How would you rate the overall implementation of the ECSM 2016 campaign (scale 1-5)?



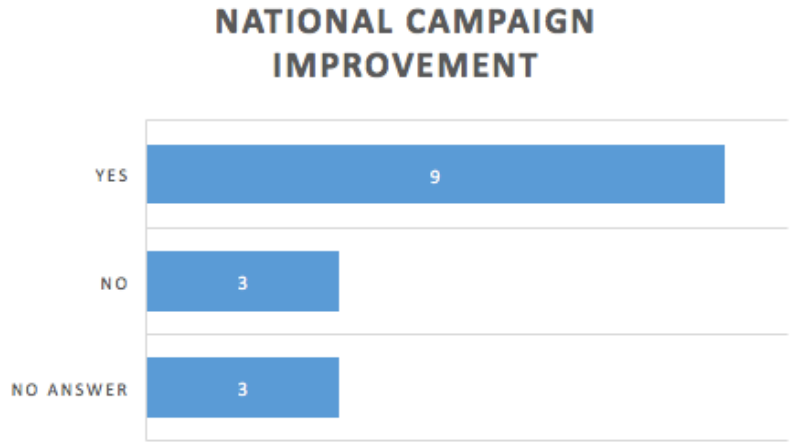
2. Did ECSM support in a satisfactory manner the outreach and promotion of your work?



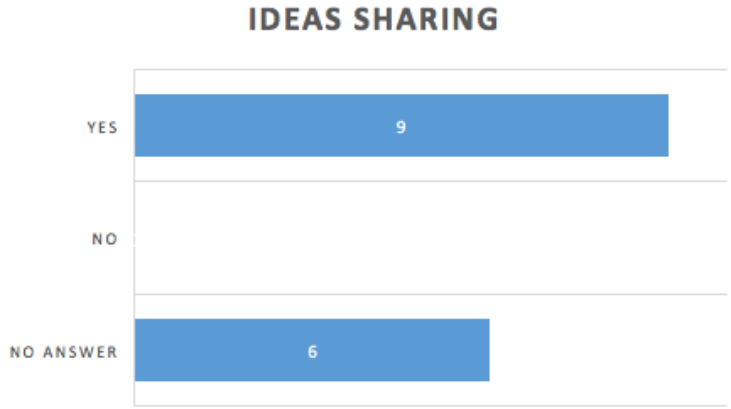
3. Did ECSM add value to your national campaign?



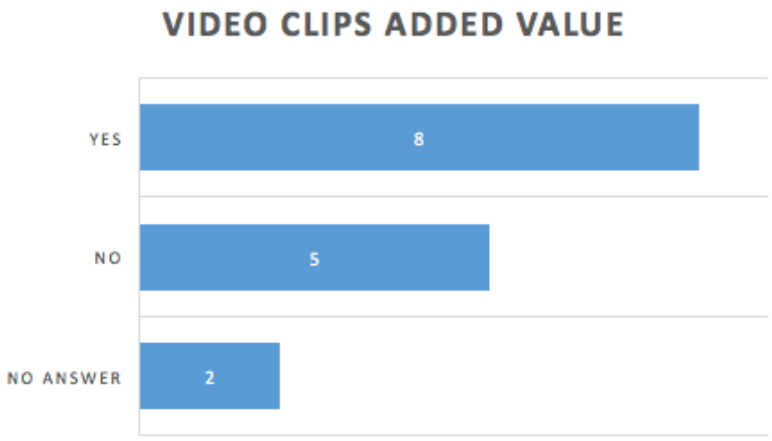
4. Did ECSM offer opportunities for improving your national campaigns through collaboration with other countries?



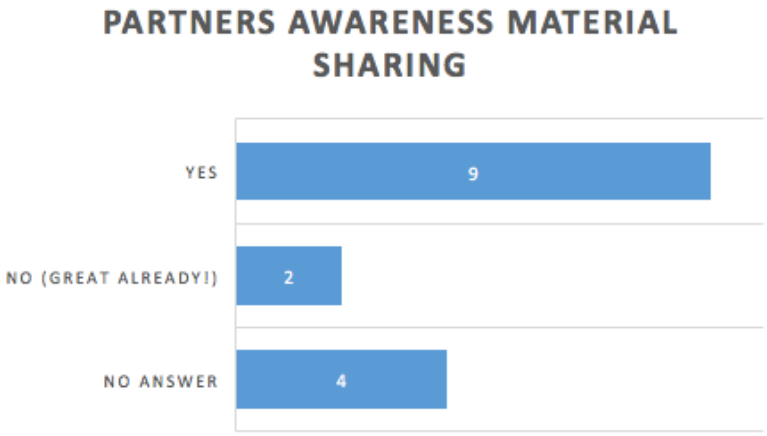
5. Do you think ENISA succeeded in the sharing and promotion of new ideas among ECSM partners?



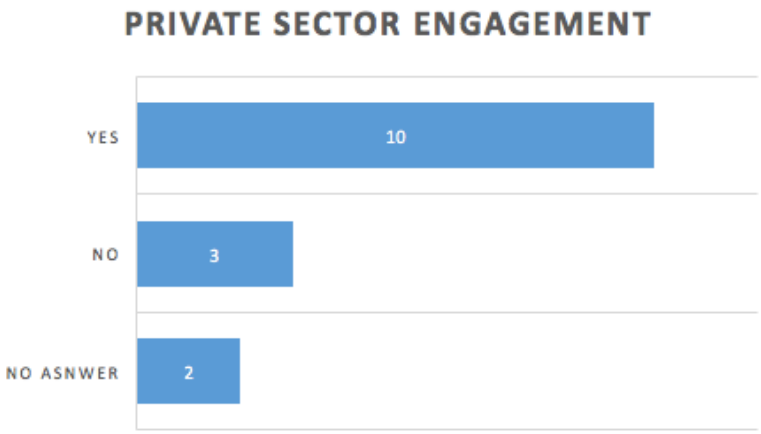
6. Did the four short video clips produced for ECSM support your national campaign?



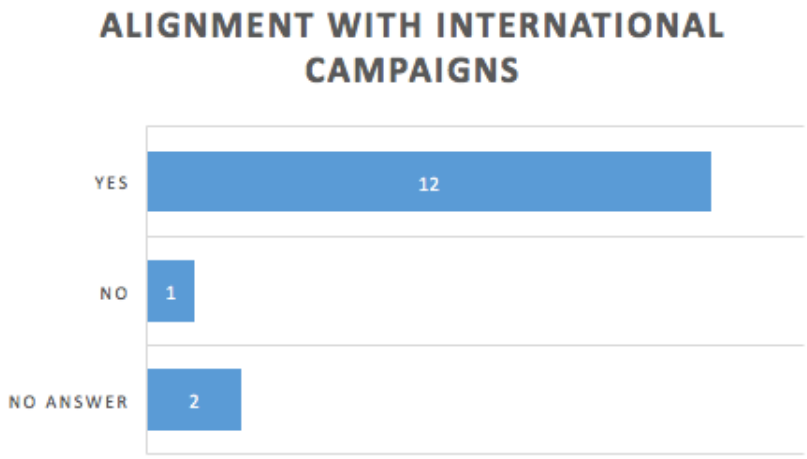
7. Could ECSM better promote the awareness material produced by its partners' campaigns?



8. Would you want ENISA to facilitate in the engagement of the private sector in future campaigns?



9. Would you want to further align ECSM with international awareness raising campaigns?



10. Do you think that ECSM offers opportunities for fostering a pan-European cyber security culture?

5.1.2 Results

MS coordinators perceived the implementation of campaign to be above average based on the results of question one. This result is significantly better than last year's results which was on the whole average.

The overwhelming majority of MS coordinators agreed that the campaign added value to their work, that it supports their local national campaigns and the promotion of their work (Q2 and Q3). Nevertheless, 40% of MS coordinators were are not entirely convinced that the campaign offered opportunities for collaboration and sharing of ideas among the MS, while on the other hand 60% believe that it did achieve these goals (Q4 and Q5).

The feedback on the short videos clips produced by ENISA was mixed with 53% supporting their usefulness to their campaigns, whilst the other half considered otherwise or did not take a position.

A large majority of MS coordinators agreed that ECSM could do better in promoting the MS awareness material. The feedback for better promotion of material included the following suggestions on how this could be achieved:

- By providing the possibility to discuss and share materials and experiences on an internal online platform/space accessible for the national coordinators (something like Basecamp, etc.)
- By better presenting such awareness material on the ECSM website
- By creating more interactions during the campaign between ENISA, the official ECSM accounts and partners
- By increasing the participation of partners and their national campaigns at the kick-off event

Feedback related to the private sector's engagement in future campaigns was positive amongst 66% of the participants however 34% rejected or hesitated to respond . A suggestion from a MS coordinator was that this should be discussed in a future ECSM meeting amongst the MS.

Finally, the majority of MS coodinators were positive about the prospect of aligning ECSM with international campaigns (Q9) and a similar results came from the question whether ECSM offers an opportunity for fostering EU-wide cyber security culture.

5.2 Web analytics

Web analytics provided the statistical data for ECSM web site and social media channels. The purpose of gathering these figures were to evaluate the impact and visibility of the campaign.

5.2.1 ECSM Web Page

The analysis takes into consideration multiple variables in relation to different types of access points to the ECSM website in the period of October.

Statistics for October include:

- ECSM page views: 92,507
- Users accessing the website: 20,486
- Total Sessions: 27,247

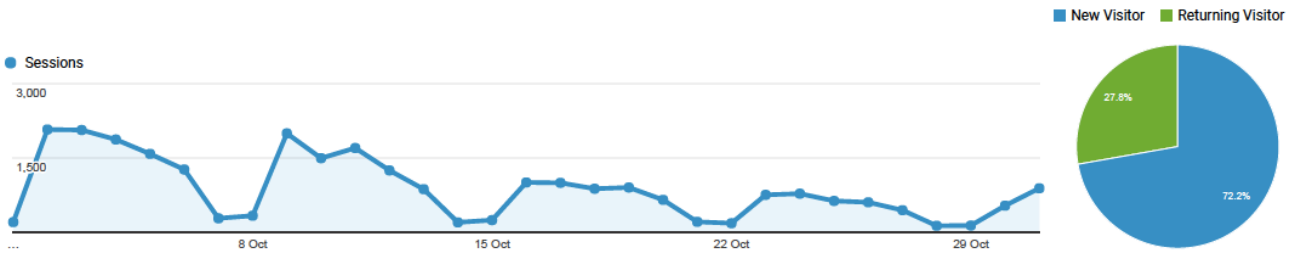


Figure 4: Graph overview of ECSM web site sessions.

The "pie" chart demonstrates the percentage of new visitors accessing the ECSM web page only once versus those revisiting the web page multiple times. While this is encouraging, ENISA recognises the need of finding the means of keeping the interest of users "alive" for a greater period of time.

Below is a comparison between this year's campaign and previous years with respect to the number of sessions and page views to the ECSM webpage. Statistics demonstrate that the ECSM website has achieved a substantial growth in its popularity in 2017 in comparison to the almost linearly increased rate of previous campaigns.

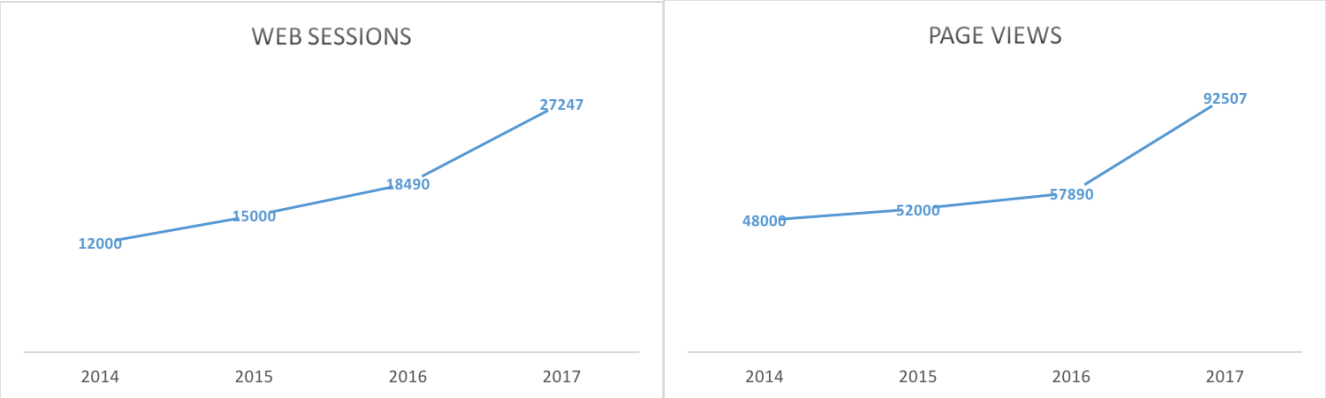


Figure 5: Overview of annual increase of ECSM web page sessions and page views

5.2.2 NIS Quiz

The data in figure 6 indicates the dispersion of page views for the NIS Quiz before during and after October. The total number of view for October reached 17,487 views out of a total of 92,507 views that the ECSM web site received in the period from 1st to 31st of October. These statistics demonstrate the popularity that the NIS quiz has gained during the campaign, equating to approximately 18,9% of the total ECSM site web traffic targeted the NIS Quiz.

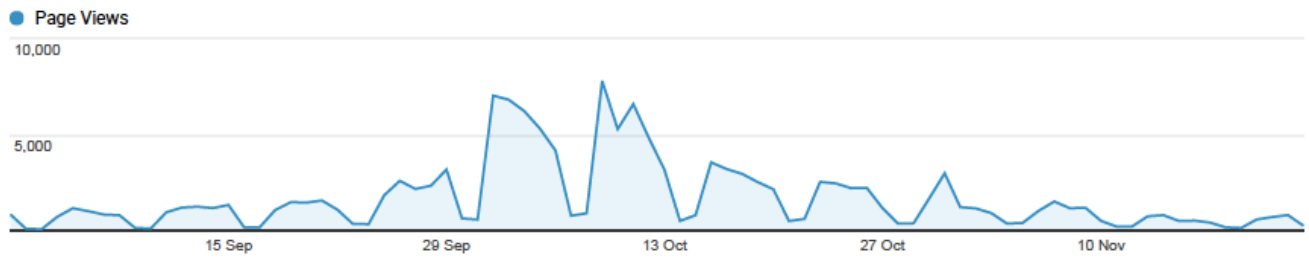


Figure 6: NIS quiz page views within ECSM October's events

The 17,487 views of the NIS Quiz can be further broken down between the views of the main page and the introductory video of the quiz as follows:

- 8,119 page views were dedicated to accessing the main NIS Quiz page
- 9,368 page views were dedicated for accessing the introductory youtube video of the quiz

The total number of visitors succeeding to complete the NIS Quiz compared to previous years increased from 788 last year to 2392 in 2017, an increase of 303%. In addition, the percentage of participants that visited the NIS Quiz home page and then went on to complete the NIS Quiz increased from 10% last year to 29.4% in 2017, reflecting that 1/3 of all visitors went on to finish the NIS Quiz.

5.2.3 ECSM Map of Activities

The following data illustrate the number of activities taking place from 2013 to 2017 during October. The graph on the left presents the total number of events registered on ECSM website during the month October every year since 2013, while the one on the right, the number of countries that have registered at least one event for the same period range.

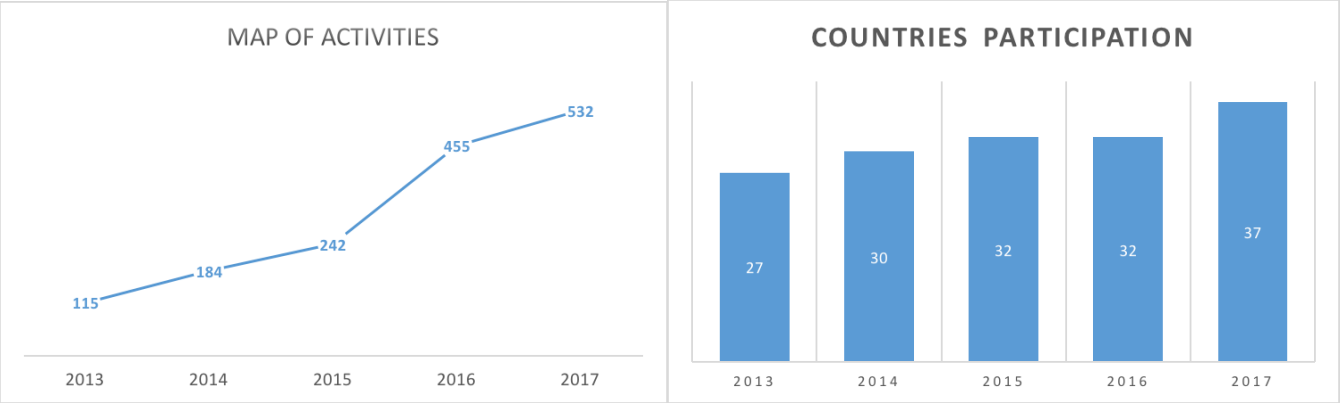


Figure 7: Number of activities in October and the number of countries registering activities annually

The rate of growth in 2017 has stabilized back to the long term average growth rate. A stable growth rate of events year on year were recorded from inception up until 2015, wherein the number of events registered almost doubled in 2016 from the previous year. The growth in the number of events registered is an outcome of the increased popularity of the campaign.

The top ten MS with respect to the number of events they have registered during October are displayed in the pie charts below for 2016 and 2017. A notable difference from last year's campaign is the Netherlands, that rose to be included in the top 5 MS with the most number of activities.

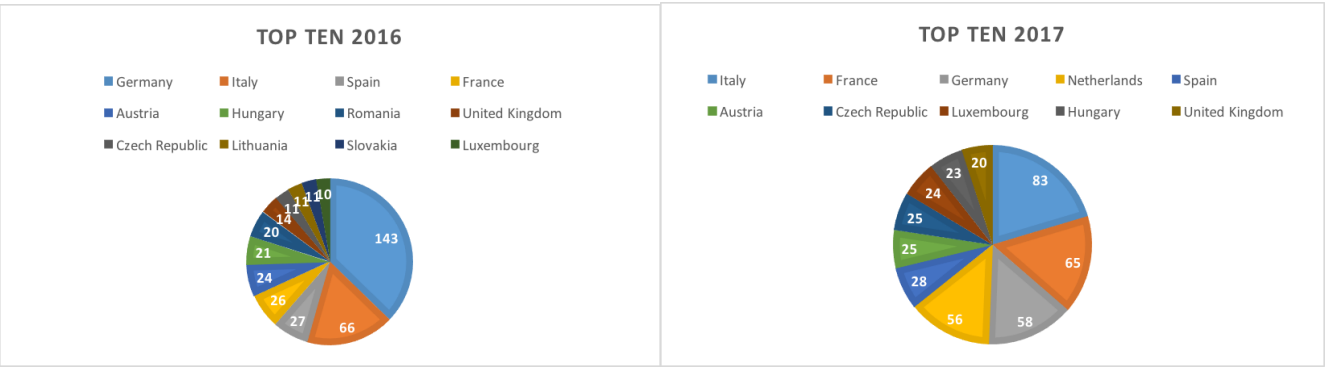


Figure 8: Top Ten countries with respect to the number of events registered for ECSM 2016 and 2017

5.2.4 Social Media

Twitter continues to support the promotion and outreach of the campaign. The figures below demonstrate the fluctuation of twitter followers from September until November 2017 for the handle @CyberSecMonth. The highest peak corresponds to the launch of ECSM and specifically the Kick-off event on the 29th of September, followed by renewed interest again until the latter end of the month.

Useful statistics that are extracted from the graph are:

- The total number of followers (12,894)
- The amount of new accounts (1,870) created within this period of three months

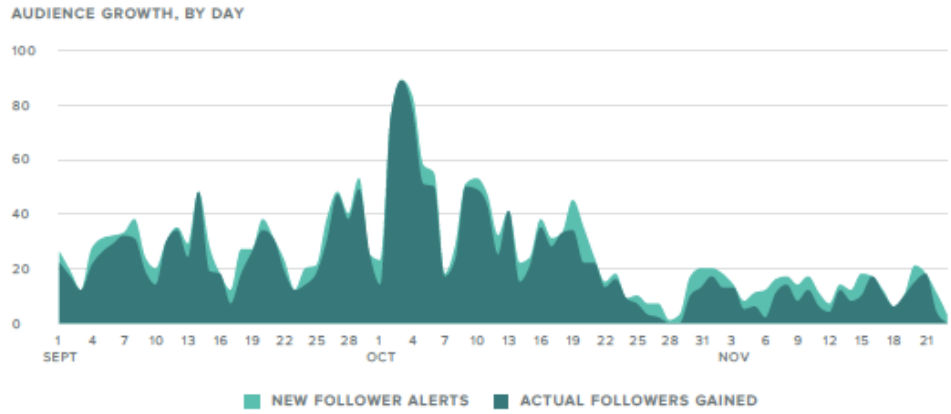


Figure 9: The daily growth of Twitter followers from September to November 2017 to @CyberSecMonth

The graph below tracks the growth in the number of twitter followers of @CyberSecMonth over time. It shows an accelerated growth in this year's campaign, almost doubling versus the pervious year.

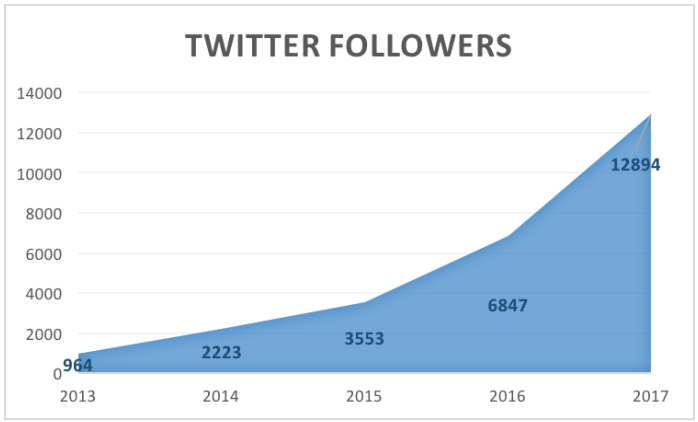


Figure 10: Annual number of Twitter followers @CyberSecMonth

5.2.5 Media Reach

There was a total of 330 articles published which mentioned ECSM from the period 23rd of September till the 7th of November. Looking at the distribution below, it can be seen that the peak of articles mentioning ECSM took place during the start of the campaign and then tapered off for the rest of the month. The online reach of the campaign, that is, the size of audience exposed to the campaign's advertisement has been estimated to be approximately 86,5m versus 112m from the previous year.

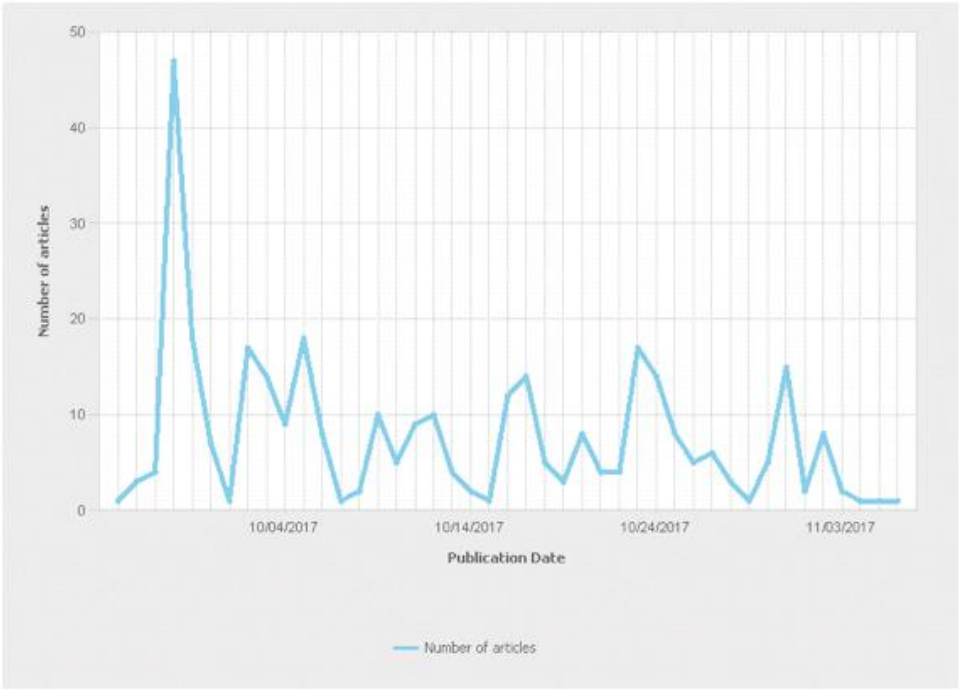


Figure 11: Number of articles published that mention ECSM from 23/09 to 7/11

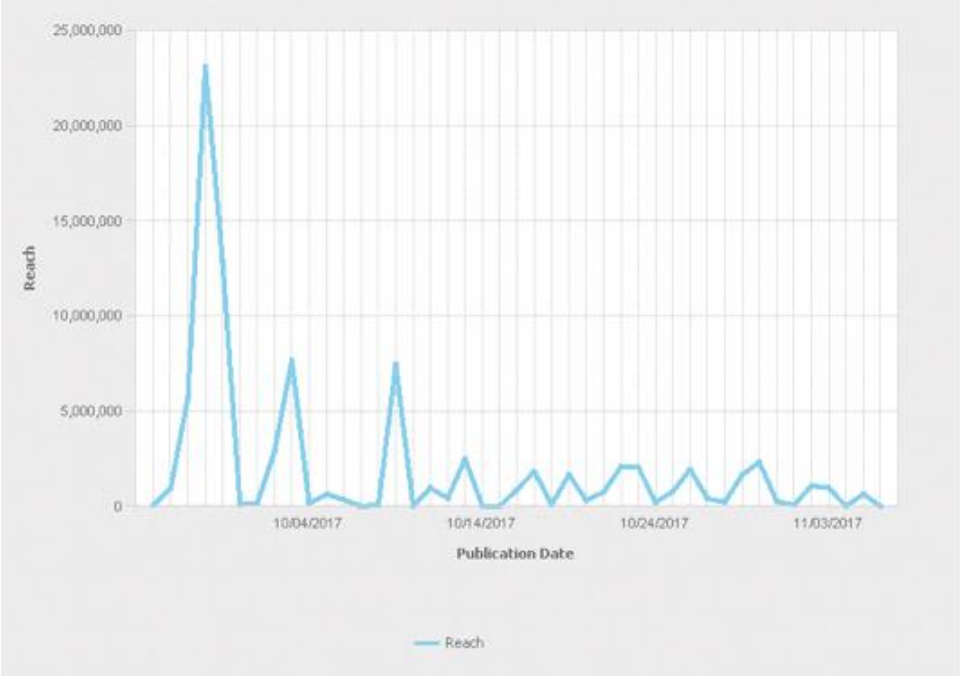


Figure 12: Estimated online reach in October 2017

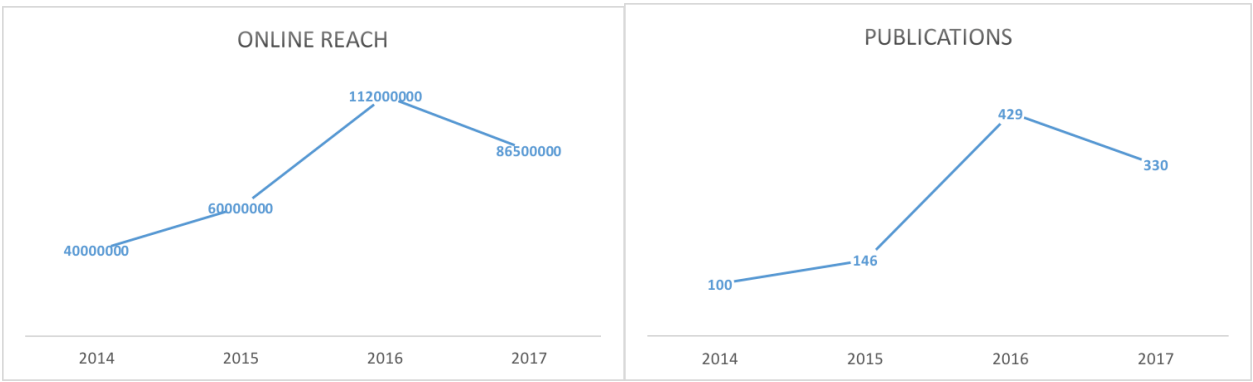


Figure 13: A comparison overview of online reach and number of articles published during October respectively

5.2.6 Conclusions

The majority of the indicators used to evaluate the campaign demonstrate a higher growth rate year on year compared to the average level of growth from previous years. In particular the growth rate of the Twitter followers and the number of participants completing the NIS Quiz (possibly triggered by EU's GDPR implementation discussions) almost doubled year on year.

Some analytics did demonstrate a minor decrease such as the online reach of the campaign and the number of publications in the period, factored possibly by the absence in this year's kick-off event of large organizations of combined resources such as the European Banking Federation (EBF) and Europol (EC3). Nevertheless, the substantial

increase of ECSM website's popularity and of the number of activities registered media followers contributed towards successful performance for the 2017 campaign.

6. Conclusions and Future Work

The performance of the campaign based on the analytical indiocators and the positive feedback received from MS coordinators confirm that the 2017 campaign succeeded to build on the results of previous years and grow inline with the long term growth rate. Several factors contributed to this positive outcome, a major one being the strength of the relationship between ENISA and the MS coordinators and another being the launch of the campaign during the EU Presidency in Estonia with the Estonian Information Systems Authority.

Another important aspect of the work carried out this year was the introduction of guidelines by ENISA to support in the organization and evaluation of the campaign. First was a set guidelines for organizing a campaign at the MS level to assist MS in the planning and execution of their national campaigns. The second was the creation of a data evaluation form to be used by MS to plan for and gather data points post the campaign at the evaluation stage. The introduction of these steps will serve to have a greater impact on future campaigns as they mature and as MS become familiar with using them.

During the course of 2017 a number of observations were made by ENISA that will be addressed in coming years so as to influence the success of the campaign going forward. These observations are listed below and include ENISA perspective on how they could be addressed.

6.1 Member State Commitment

Member States participate on a voluntary basis in the organization of the campaign. Participants are predominantly representatives from the National Cyber Security Centres, responsible Government Ministries or the CERT community. Some Member States have dedicated units and personnel whilst others work on a best effort basis alongside their other core activities.

There are a dozen or so core participants to ECSM from the Member States that actively participate in the monthly conference calls and physical meeting. The remaining Member States participate on an ad hoc basis or not at all.

EU Member States participating: Austria, Czech Republic, Estonia, Finland, France, Germany, Hungary, Luxembourg, Netherlands, Norway, Poland, Romania, Slovenia, Switzerland

'Passive' participation: Belgium, Bulgaria, Greece, Latvia, Lithuania, Malta, Portugal, Spain, Sweden, UK

EU Member States not participating: Croatia, Cyprus, Denmark, Ireland, Italy, Slovakia

From ENISA's perspective all Member States should be actively participating in the campaign. ENISA will demonstrate to the MS the advantages of being involved in the campaign and the effectiveness of working together to increase impact. In many cases lack of financial resources is identified by MS as the main reason for little contribution to the ECSM activities or no participation.

6.2 Private Sector Involvement

Private sector involvement has been limited to participation of speakers / panellists during the annual Kick-Off event that launches the activities of ECSM. Discussions were held with Member States to enhance the engagement of the private sector in the campaign either via jointly producing material or promoting the activities via their media channels or by sponsoring activities, however consensus among the Member States was not reached and discussions were postponed until the next face to face meeting in February 2018.

From ENISA's perspective industry involvement is critical in promoting the campaign and disseminating the messages to a wider audience. There is keen interest from industry to be involved, the question is; What is the ideal model for guiding this relationship?

The latest Joint Commission of the European Parliament and Council[12] emphasized the strong role for the industry in this endeavour and gave particular attention to digital service providers and manufacturers: "It (industry) needs to support users (individuals, businesses and public administrations) with tools that allow them to take responsibility for their own actions online, making clear that maintaining cyber hygiene is an indispensable part of the offer to consumers".

6.3 Governance Structure

The campaign has been prominently driven by ENISA (with the role of secretariat, 'facilitator') over the past five years; with Member States participating on a voluntary basis with the majority acting as observers rather than active participants.

Involvement of the Member States consists of providing input into the monthly conference calls and participating in the annual physical meeting. The agenda for these meetings are prepared by ENISA and input is requested of the Member States on decisions concerning the themes of the month, production of dissemination material, functionality of the website, the kick-off event and other tactical aspects of the campaign.

From ENISA's perspective a governance structure must be created to drive the decision making processes and the responsibilities of the Member States. However this would require a commitment from the Member States, especially those that take up an active role within the existing decision making structure. Given the current level commitment of the Member States only a handful would have the capability to take up such a role.

For example, a similar governance structure could be created to that of the CSIRT Network; in which the current EU Presidency chairs and the past and future EU Presidency co-chair the steering committee, with the Member States including the EC have voting rights. Working groups would be created within this structure to tackle certain aspects of the campaign. The role of the Agency would be to act as facilitator and advisor to the group.

6.4 Collaboration with the European Commission

The European Commission (EC) so far supports the campaign mainly through hosting and participating at the annual physical ECSM meeting, participation of senior officials at the launch event and translation of the annual press release and NIS Quiz in 2016.

In 2017 the European Commission introduced the concept of "Cyber Security Ambassadors". Its main aim is to inform European Commission officials about the important Cyber Security European Commission achievements regarding policies (e.g. Cyber Security Package, Prize), legislation (NIS, GDPR), training efforts (ENISA, EC – Cyber Aware and CNECT University), operations (CERT-EU) and campaigns such as the ECSM, EU Code Week, etc. In this context, European Commission staff who are willing to perform as Ambassadors in the European setting are expected to promote the European Commission Cyber Security efforts in contacts outside the EX, strengthen the presence of the European Commission and support European citizens and organizations in their Cyber Security awareness efforts by

[12] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017JC0450&from=EN

providing information and advice. ENISA actively supported this initiative and will continue to do so by preparing and update relevant dissemination material.

From ENISA's perspective the support of the European Commission for ECSM could be stepped up in a number of ways, such as for a permanent European Commission representative to be involved in the steering of the campaign via the monthly conference calls and physical meeting. The European Commission could use its privileged position to outreach to communities and stakeholders, to garner support and help promoting the campaign. Another aspect to this is the visibility of the kick-off event, that would be greatly impacted by the attendance of a Vice President or Commissioner, for which the EC could play a pivotal role in securing. Finally, the commitment to the campaign from the Member States could be stepped up with the right message from the right officials within the European Commission.

6.5 International Collaboration

Cyber Security campaigns aimed towards citizens is now a global phenomenon, with the majority of developed nations campaigning; particularly in October.

In the 2013 Cybersecurity Strategy of the European Union[13] the EC invited the Member States to organize a yearly campaign, with the support of ENISA and included a recommendation to synchronize the EU-US cybersecurity month starting 2014. The Working Group, established at the EU-US Summit[14] [15] in November 2010 is tasked with developing collaborative approaches in cyber security, including efforts towards a programme of immediate joint campaigns activates as well as a roadmap towards synchronized annual awareness efforts. In this respect some small steps have been taken to align and cross promote the campaign themes and messages with that of the U.S. but with further willingness from both parties a fully synchronized campaign could be achieved in the coming years.

From ENISA's perspective synchronizing with the U.S. would further strengthen the campaign's outreach and promotion, and would widen the portfolio of materials available to citizens. However, synchronizing with the U.S. is not the end goal; the end goal is to synchronize the campaigns globally into a unified message that resonates beyond boarders. In that case is probably worth to consider the current timing of ECSM during the month of October. If the collaboration between Europe and the USA in the context of ECSM is not considered as a priority for the future, perhaps we should consider shifting the ECSM activities towards spring or early summer avoiding the period of July-August (just before the ECSM) that poses organisational problems.

6.6 Annual ECSM Launch Event

The annual kick-off event to launch the campaign has had mixed results over the years. However due to the collaboration with authorities in the hosting MS in 2017 and with the industry in 2016, the participation was higher than average and attracted a number of high profile panellists. This development indicates that the event is sustainable only with the support of another co-organizer and that it has not matured enough to stand on its own, as yet.

[13] http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[14] http://europa.eu/rapid/press-release_MEMO-11-246_en.htm

[15] http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

The next steps in the evolution of the campaign is to reassess the goal and scope of the kick-off and re-examine the input from the Member States, EC and the private sector.

From ENISA's perspective the kick-off event requires the support of a prominent European figure to give it visibility and a reassessment of the goals and scope is needed if it is to continue.

6.7 Website Redesign

The ECSM website has served the campaign well over the past 5 years. Certain features have been enhanced and webpages were added to streamline the experience for the user. The main goal of the website is to inform the general public of events that occur in their area and to provide them with tools needed to protect themselves online, such as recommendations and the NIS Quiz. The website also acts as a depository of material from all the Member States and from European Institutions such as Europol. This allows campaign coordinators from the Member States to re-use material that have been created by others that they are focusing on at the National level. ECSM website also seeks to drive traffic to the Member States relevant campaigns and includes a dedicated supporters page. One may argue that the ECSM may be used as an information resource also targeted towards the citizens. As it is depicted in the graphs of Annex A the uptake of the ECSM social media channels is very good indicating that they are a better path towards the EU citizens. In this respect, ENISA will continue investing on the use of the ECSM social media channels.

[3] http://europa.eu/rapid/press-release_MEMO-11-246_en.htm

[4] http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

Annex A: Kick-Off Event Agenda

ECSM Kick-Off Event Agenda
29th Sept 2017
Mektory, Raja 15, 12618, Tallinn, Estonia

ECSM Kick-Off Event Agenda

TIME	TOPIC	SPEAKERS
09.00 – 09.30	Registration	
09.30 – 09.35	Welcome	Taimar Peterkop, Director General, RIA
09.35 – 10.00	Welcome speeches	Andrus Ansip, Vice President of the European Commission (Tentative) Despina Spanou, Director, DGCNECT, EC Udo Helmbrecht, Executive Director, ENISA Ken Ducatel, Director, DIGIT, EC
10.00 – 10.30	ECSM Campaign	Moderator: Vangelis Stavropoulos, ECSM Project Coordinator, ENISA Estonia: Klaid Magi, Head of CERT EE France: Anne-Charlotte Brou, Agence Nationale de la securite des systems d'information (ANSSI) Germany: Hanna Heuer, Federal Office for Information Security (BSI) Luxembourg: Daniele Bisdorff, Ministere de l'economie du Luxembourg
10.30– 11.10	Cyber Security in the Workplace	Moderator: Lauri Almann, BHC Laboratory Karlis Podins, Threat Analyst, CERT.LV Kai Roer, Founder, CLTRe Christos Sgaras, Senior Information Security Specialist, Europol Zinaida Benenson, Senior Researcher, University of Erlangen-Nuremberg
11.10 - 11.25	Break	
11.25 – 12.05	Cyber Security in the Home	Moderator: Claire Vishik, Senior Director, Global Cybersecurity, Intel Peter Cassidy, Co-Founder of STOP. THINK. CONNECT. Messaging Convention William O'Connell, Chief Business Security Officer, ADP Anthony Grieco, Trust Strategy Officer, CISCO
12.05 – 12.45	Skills in Cyber Security	Moderator: Demosthenes Ikonomou, Head of Operational Security, ENISA Olaf Manuel Maennel, Professor Department of software science, TTU John De Santis, CEO, Hytrust Alexandra Maniati, Senior Policy Adviser, European Banking Federation
12.45 – 13.00	Closing Remarks	Andrus Ansip, Vice President of the European Commission (tentative) Udo Helmbrecht, Executive Director, ENISA
13.00 – 14.00	Networking Lunch	

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710 | info@enisa.europa.eu | www.enisa.europa.eu

Annex B: Evaluation Data Collection Form

This document aims to collect evaluation data by Member State Coordinators regarding each ECSM activity that they organize. Please complete for each ECSM activity the relevant information.

Country (Member State) Name:	
Organization Name:	
Acronym:	
Email:	
Website:	

Conference/ Workshop activities

If you organized an ECSM conference/workshop, please respond to the below inquiries. If you organized more than one conferences, please copy the Table for as many times as needed to provide answers for each activity.

Evaluation Metric	Response
What was the duration of conference/workshop? (in days)	
How many people attended the conference/workshop?	
What was the opinion of the attendees about the conference/workshop?	
How many security themes were covered? Please enlist them.	
What were the target audience groups? Please enlist them.	
What was the total cost of the conference/workshop organization?	

TV or Radio Advertisement activities

If you organized an ECSM TV or radio advertisement, please respond to the below inquiries. If you organized more than one TV or radio campaigns, please copy the Table for as many times as needed to provide answers for each activity.

Evaluation Metric	Response
How many times was the advertisment displayed (number of impressions)?	
What was the duration of the advertisement? (in seconds)	
In how many TV channels and/or radio stations was the advertisement displayed?	
What was the total cost for the advertisement campaign?	

Website

If you are holding an ECSM related website, please respond to the below inquiries. If you are holding more than one ECSM related websites, please copy the Table for as many times as needed to provide answers for each website.

Evaluation Metric	Response
How many people have visited the website?	
How many people have visited the website during ECSM 2017?	
What is the average time that the visitors spent on the pages of the website (Time on Page)?	
What is the percentage of visitors to the website who entered and then left without clicking to anywhere else on your website (Bounce rate)?	
What is the number of unique visitors of your website?	

What is the total number of actions (e.g., page view, registrations, form submissions) occured on the website by the visitors?	
What is the average time the webpages were viewed by the visitors (Page view duration)?	
What is the average time the visitors actually interact during the page viewing (Active time)?	

Social Media Activities

If you holding an official ECSM related social media account please respond to the below inquiries. If you are holding more than one social media accounts, please copy the Table for as many times as needed to provide answers for each account.

Evaluation Metric	Response
If it is a Facebook account, what is the average number of 'Likes' for posts?	
If it is a Facebook account, what is the average time that people share posts?	
If it is a Facebook account, what is the number of Followers?	
If it is a Facebook account, what is the Organic Reach for each #ECSM related Post?	
If it is a Facebook account, what is the Paid Reach for each #ECSM related Post?	
If it is a Facebook account, what is the total Reach for each #ECSM related Post?	
If it is a Tweeter account, what is the number of Followers?	

If it is a Tweeter account, what is the average number of retweets for each #ECSM Tweet?	
If it is a YouTube account, what is the average number of views per uploaded video?	
If it is a YouTube account, what is the average view duration per uploaded Videos?	

Fair Stand/ Exhibition and Roadshows

If you participated in fair stands, exhibitions or roadshows to promote security awareness please respond to the below inquiries. If you participated in more than one fair stands, exhibitions or roadshows, please copy the Table for as many times as needed to provide answers for each activity.

Evaluation Metric	Response
How many locations did you visit through the fair stand, exhibition or roadshow?	
How many people visited the stand, exhibition or roadshow?	
How many people visited the ECSM booth?	
What was the total cost for participating at the stand, exhibition or roadshow?	

Merchandising, Posters, Leaflets

If you produced promoting material please respond to the below inquiries.

Evaluation Metric	Response
How many units of materials were distributed?	
In how many cities or locations was the material distributed?	
What was the total cost for material development and distribution?	

Tests/Quizzes

If you organized tests and quizzes within ECSM please respond to the below inquiries. If you organized more than one tests/quizzes, please copy the Table for as many times as needed to provide answers for each activity.

Evaluation Metric	Response
How many people took the test/quiz?	
How many people who took the test/quiz, retook it?	
What is the average performance of the participants?	

ECSM Organization Effort

Evaluation Metric	Response
How many persondays/personmonths were allocated by your organization for ECSM 2017?	
How many full time employees worked for ECSM 2017?	

Annex C: Guidelines for Data Collection Form

Background Information

This document is developed by ENISA to assist the EU Member State Coordinators with the design and implementation of their awareness raising campaigns within the scope of the European Cyber Security Month (ECSM). This document reflects the effort of ENISA to support EU Member States, through guidelines for the preparation of ECSM evaluation. This document is complementary to the document 'ECSM 2017 Guidelines for the Member State Coordinators' that was published on April 2017. Section 2 presents the evaluation metrics per activity expected per EU Member State participating in ECSM and Section 3 presents aggregative evaluation metrics for ECSM in Europe.

Proposed Evaluation Metrics per Activity Type

In this document ENISA offers to the EU Member State Coordinators recommended evaluation metrics in accordance to the type of awareness activity that is performed each time. Awareness activities within ECSM may include conferences, seminars, workshops, events, social media campaigns, merchandising, and others (ENISA, 2011). Depending on the type of the awareness activity, different evaluation metrics to measure the effectiveness can be applied, as displayed in the Table below.

Activity Type	Recommended Evaluation Metrics	Description of Preparation Activities	Documentation
A. Conference/ Workshop	A1. Number of attendees	A registry of participants during the conference/workshop (anonymous or with name)	Registry of participants (e.g., 75 people attended the conference)
	A2. Participant's Opinion	Designing a questionnaire for collecting participants' feedback and distribution after the conference/workshop	Completed questionnaires (e.g., average satisfaction level)
	A3. Security Themes covered	List of the security themes covered or conference/event program	Conference/ Workshop Program (e.g., malware and social engineering themes)
	A4. Target Groups	List of the target groups	Conference/ Workshop Program (e.g., citizens, business users)
	A5. Cost	Total cost of conference/workshop	Cost amount (e.g., 3.000 Euros)
B. TV or Radio Advertisement	B1. Number of Impressions	Recording of the times the advertisement is displayed	Number of Impressions (e.g., 1000 impressions during ECSM)
	B2. Duration of Advertisement	Recording of the advertisement duration	Duration (e.g., 12 seconds)

	B3. Number of Channels	Recording of the number of radio or TV channels	Number of Channels (e.g., 3 radio channels)
	B4. Cost	Total cost of advertisement	Cost amount (e.g., 2.500 Euros)
C. Website	C1. Number of Visitors	The number of unique people who visited the website	Log files or cookies (e.g., 540 visitors)
	C2. Number of Cisitors during ECSM	The number of unique people who visited the website during ECSM	Log files or cookies (e.g., 240 visitors)
D. Social Media	D1. Number of 'Likes'	The number of unique people who 'Like' the Facebook page	Social media reporting (e.g., 455 Likes)
	D2. Number of 'Shares'	The number of times that national ECSM activities are shared	Social media reporting (e.g., 230 Shares)
	D3. Number of Followers	The number unique people who 'Follow' the updates of Twitter	Social media reporting (e.g., 300 followers)
	D4. Number of Tweets and retweeted	The number of times that an ECSM Tweet is retweeted	Social media reporting (e.g., 50 tweets, 170 retweets)
	D5. Number of video views	The number of unique people who viewed the Youtube video	Social media reporting (e.g., 13.234 views)
E. Fair Stand/ Exhibition and Roadshows	E1. Number of locations visited	A registry of locations	Registry of locations (e.g., 5 cities)
	E2. Number of event visitors	The number of visitors who attended the Fair Stand, Exhibition or Roadshow	Fair Stand, Exhibition or Roadshow statistics (e.g., 120.000 visitors)
	E3. Number of booth visitors	The number of people who visited the national campaign booth	Registry of visitors (e.g., 700 visitors)
	E4. Cost	The booth and registration cost	Cost amount (e.g., 4.500 Euros)
F. Merchandising, Posters, Leaflets	F1. Number of units of materials distributed	The total number of units of materials distributed	Number of units (e.g., 150 leaflets)
	F2. Number of cities/ locations	The number of cities or locations where material was distributed	Number of locations (e.g., 3 cities)
	F3. Cost	Total cost of material development and distribution	Cost amount (e.g., 1.500 Euros)
G. Tests/Quizzes	G1. Number of participants	The number of unique people who took the test/quiz	Test or Quiz statistics (e.g., 35 participants)
	G2. Number of retakes	The number of people who retook the test or quiz to check their improvement	Test or Quiz statistics (e.g., 10 retakes)
	G2. Performance	The average performance of the participants	Test or Quiz statistics (e.g., 6.5/10)

Aggregative Evaluation Metrics

The below evaluation metrics will be used for the assessment of each ECSM and overall ECSM in Europe.

Recommended Metric	Description of Preparation Activities
Number of activities	Calculated by ENISA provided that all EU Member State Coordinators will complete the ECSM activities template
Number of security themes	Calculated by ENISA provided that all EU Member State Coordinators will complete the ECSM activities template
Number of Languages	Calculated by ENISA provided that all EU Member State Coordinators will complete the ECSM activities template
Number of Delivery Channels	Calculated by ENISA provided that all EU Member State Coordinators will complete the ECSM activities template
National Preparation Effort	Number of persondays/personmonths per EU Member State Coordinator (e.g., 35 persondays allocated to ECSM) Number of full time employees (e.g., 3 full time employees worked for ECSM)
ECSM Preparation Effort	Calculated by ENISA provided that all EU Member State Coordinators will offer own information
Social Media Exposure	Calculated by ENISA and the social media analysis partner
ECSM Website Exposure	ENISA will calculate the number of unique people who visited the website

Annex D: Guidelines for Member State Coordinators

Background Information

The European Cyber Security Month (ECSM) is an EU advocacy campaign that promotes cyber security among citizens and advocates for change in the perception of cyber-threats by promoting information security and sharing of good practices and competitions. The European Union Agency for Network and Information Security (ENISA), the European Commission DG CONNECT and Partners are deploying the European Cyber Security Month (ECSM) every October.

The European Cyber Security Month aims at generating general awareness about cyber security; generating specific awareness on Network and Information Security (NIS); promoting safer use of the Internet for all users; building a strong track record to raise awareness through the ECSM; involving relevant stakeholders; increasing national media interest through the European and global dimension of the project; and enhancing attention and interest with regard to information security through political and media coordination.

This document reflects the effort of ENISA to support EU Member States on the design and implementation of national European Cyber Security Month campaigns, though guidelines.

1.1 ENISA's Vision for ECSM 2017

The vision of ENISA for ECSM is to support the EU Member States with the design and implementation of their awareness raising campaigns and to promote collaboration among EU Member States, international organizations and industry.

1.2 ENISA's Mission statement for ECSM 2017

ENISA's mission is to collaborate with the EU Member States and international organizations by finding innovative and fun ways to raise EU citizens' awareness of cybersecurity, be they by organizing events, conferences, online quizzes, transferring of best practices or the use social media to educate and inform the public. Our mission is to enhance the delivery and synchronize ECSM among the EU Member States and industry that will share a pan-European vision and values for cybersecurity.

2 Guidelines for Planning European Cyber Security Month

2.1 A common Understanding of Security Awareness

To develop effective ECSM campaigns with pan-European coverage, EU State Members should share a common understanding of the concept of security awareness. For this purpose, this document presents widely accepted definitions of information security awareness.

Information security awareness is usually associated with organizational contexts and is part of a broader information security communication framework. ENISA (2010) defines security awareness as a "component of the education strategy of an organization which tries to change the behavior and patterns in how targeted audience (e.g. employees, public, etc.) use technology and the Internet and it is a distinct element from training. It consists of a set of activities which turn users into organizations' first line of defense… awareness activities occur on an ongoing basis, using a variety of delivery methods and are less formal and shorter than training" (ENISA, 2010, p. 15). NIST special publication (NIST, 2003) states that information security awareness aims at instilling a common understanding of information security concepts and topics; covers a

broad audience of users; relies on attractive packaging techniques and is expected to bring short-term results. Maeyer (2007) defines security awareness as “an organized and ongoing effort to guide the behavior and culture of an organization with regards to security issues”. Thomson and von Solms (1998) state that security awareness is “about making users aware of the value and importance of information and security procedures”. Information security awareness aims at a state in which “users would intuitively act towards protecting information security”, when processing information with information systems and tools. An information security awareness program aims at transiting from users’ “ad-hoc secure behaviors to constant secure behaviors” (Okenyi and Owens, 2007). In organizational contexts, security awareness has been highly associated with users’ compliance to information security policies (Bulgurcu et al., 2010; Yang et al., 2011; Haeussinger and Kranz, 2013; Talib and Dhillon, 2015). Regardless of their differences, these definitions reflect a common concept surrounding security awareness: the target to attract the attention of users to security messages, to make them understand the importance of information security and their potential security obligations. Also, it is generally accepted that security awareness is associated with some form of users’ behavioral change (Albrechtsen, 2008; ENISA, 2010; Okenyi and Owens, 2007; Tsohou et al., 2015).

Recently, information privacy became an essential component of users’ awareness, when handling digital services; especially with regards to protecting their personal information. For that purpose, this document also presents prevailing definition on what constitutes general privacy awareness to inform the Member State Coordinators of ECSM campaigns.

Information privacy awareness is defined as “someone's ability to accurately perceive potential privacy threats” (Könings et al, 2013, p.164). In another definition privacy awareness “measures the awareness of Internet users regarding a general existence and possibility of Internet privacy issues, without focusing on technical details or on a user” (Brecht et al., 2012 p.3). Cetto et al. (2014, p. 2) state that privacy awareness is “an individual's knowledge of who can access which shared personal information and moreover, the degree to which actual and perceived visibility of shared items match”. Malandrino et al. (2013, p.2) refer to privacy awareness as “perception of: 1) Who is tracking, receiving or collecting private information (2) When information is collected (3) What information other entities receive, store and use (4) How pieces of information are processed, linked and aggregated to potentially build detailed users' profiles”. Information privacy awareness is also considered as “user's attention, perception and cognition of whether others receive or have received personal information about him/her, his/her presence and activities, which personal information others receive or have received in detail, how these pieces of information are or may be processed and used, and what amount of information about the presence and activities of others might reach and/or interrupt the individual” (Pötzsch, 2009, p. 228). Information privacy awareness has also been widely associated with the terms of use and privacy settings of online contexts, such as social media (Moey et. Al., 2016; Sohoraye et al., 2015; Kuo and Talley, 2014; Bergmann, 2009).

Based on the above analysis, we formulate the following first guideline for the Member State Coordinators of ECSM campaigns.

Guideline 1: Member State Coordinators are encouraged to create campaigns aiming at activating users to protect information from security threats. Campaigns are expected to attract recipients’ attention and make them recognize information security concerns and respond accordingly. ECSM campaigns should also strengthen users’ abilities to accurately perceive potential privacy threats, with regards to their shared personal information.

2.2 Formulation of Project Plan

Developing the yearly ECSM campaigns requires proper formulation of a project plan, including specifying the ECSM team, their roles and responsibilities, the budget, ECSM activities, milestones, timeline and deadlines.

When specifying the budget, the Member State Coordinators should consider personnel costs, operational costs, advertisement costs, any technical development and support costs. While considering the costs of an initiative, the possible contribution of third parties should be considered. This is valid when an information security awareness program is part of a public–private partnership (ENISA, 2010).

It is important to produce a documentation of the overall project plan, given that ECSM is a yearly initiative. The future event coordinators will find the documentation invaluable.

Guideline 2: Member State Coordinators are recommended to develop an ECSM project plan that can guide the management of all involved activities for design, execution and evaluation. It is imperative to produce a documented project plan.

2.3 Definition of Communication Plan

In the early stages of a security awareness campaign design it is imperative to define the target group or groups (ENISA, 2010; NIST, 2003).

There are several potential recipients and categories of recipients that a security awareness campaign may target, such as home users, adults, citizens, employees, parents, public officers, teenagers, Internet users (ENISA, 2011). Obviously, there is an overall between these categories, and this is one reason why it is crucial to identify clearly defined target groups. More importantly, it is necessary to recognize and separate target groups, because society consists of a diverse collection of individuals with differing interests, levels of expertise and priorities (ENISA, 2010); thus, it is difficult to find issues and messages that will be relevant to everyone.

ENISA (2011) offers a useful categorization that can be valuable to the Member State Coordinators, which separates three broad categories of recipients: general users, young people and business users.

Category of Users	Description
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

Guideline 2: Member State Coordinators need to clearly define the target group or groups of ECSM national campaigns. The Member State Coordinators can broadly separate target audience into general users, young people or business users. The design of the ECSM campaigns should be customized upon the defined target groups.

The communication channels that will be used for delivering security awareness are a critical success factor.

Some key recommendations for an effective awareness campaign are:

- Reach out to as broad an audience as possible
- Use influential and credible communication channels and senders of messages
- Use more than one communication channel to engage the recipients successfully

Traditional communication channels (ENISA, 2010; NIST, 2003) that can be used are: brochures, leaflets, comics, screensavers, newsletters, posters, emails, events, puzzles, do and don't lists, emails, radio or TV, SMSs, website.

The Member State Coordinators are encouraged to also consider innovative communication means, which may increase the possibilities of success. Mobile applications that offer notifications to the enrolled users, and may enhance the engagement of the users given the ongoing nature of the ECSM communication (ENISA, 2011, p.35). Another option may include online games (Cetto et al., 2014; Cone et., 2007; Albrechtsen and Hovden, 2010), which can provide personalized content and tailor the presented context and security challenges to the user's past performance.

Communication channels should be chosen taking into consideration the type of target group, its profile, as well as information technology and security knowledge.

Guideline 3: Member State Coordinators should choose to use multiple communication channels reaching out for broad audiences and sending awareness messages from credible and influential sources. Communication channels can be chosen from several traditional communication channels available, but innovative communication channels are highly encouraged.

Defining the security messages that will be presented to the audience is a critical activity of the ECSM campaign design. Common information security awareness themes (ENISA, 2010) are security threats in e-mail and electronic communication, password protection, information security policies and procedures and security incident reporting (for business users), website policies, social engineering, etc.

Information security themes, however, should be chosen based on the current trend of information security and privacy threats, to deliver timely guidance to the users. The Member State Coordinators are encouraged to study the recent landscape of security and privacy threats, before deciding the themes of the ECSM 2017 campaigns. For example, ENISA (2017) has identified the top cybersecurity threats for 2016. In priority, the top ten threats include malware, web-based and web application attacks, denial of service, botnets, phishing, spam, ransomware, insider threat, physical damage/theft. In terms of information privacy Unesco (2012) highlights that high privacy threats relate to user identification, adware, spyware and malware, data logging and surveillance, deep packet inspection, location-based services and surveillance and Internet surveillance technologies generally. Individuals are now using modern technologies and security awareness campaigns should keep pace with the technological platforms that are interesting to them and present relevant security themes; trends such as Internet of Things, advanced authentication, cloud computing, mobile applications, mobile payments, big data, bring your own device (PwC, 2016). Given that ECSM activities spread in a period of a month the Member State Coordinators can specify few security themes and divide them across the ECSM; e.g., week 1 may focus on Internet of Things security, week 2 may focus on bring your own device security, etc.

Guideline 4: Member State Coordinators are encouraged to choose information security themes addressing both a) commonly identified security threats, and b) threats identified by national or international classifications as current security threats.

Guidelines for Evaluating European Cyber Security Month

3.1 Evaluation Approaches

The evaluation of a security awareness program is a challenging task. Literature includes different approaches on how the success of such a program should be measured. For example, one category of evaluation approaches tests the participants' awareness through questionnaires; the participant is requested to complete the questionnaire before the awareness program and following the awareness program, and it is expected that awareness level will be raised. In this category, Parsons (2014) created a questionnaire that can be used to evaluate an employee' s security awareness. The questionnaire tests the awareness of an employee on common security threats, such as password management, email use, Internet use, incident reporting, mobile computing, etc. Similarly, Kruger and Kearney (2006) developed a questionnaire to test an individual's security awareness, which can be automated and customized based on the needs of the evaluators. However, this evaluation approach is not suitable for the ECSM participants, given that the respective awareness events target broad audiences, such as the public.

ENISA (2010), offers a more holistic approach offering various awareness evaluation metrics for different audiences:

- Evaluation at the business layer measures the impact of the overall project
- Evaluation at the service layer measures the awareness activities output
- Evaluation at the operational layer measure the awareness processes

Examples of the evaluation metrics per layer are given below:

Layer	Indicative Metrics
Business	number of events listed/month, number of material distributed/edition, number of material distributed/year, number of people attending awareness trainings per campaign, number of unique visitors/month, time to organize an awareness initiative
Service	number of topics on security in standard primary and secondary school education/total topics, number of topics on security in high school and education/total topics, number of e-government projects using standards/total projects
Operation	mean time between discovery and notification of a new threat, number of reported incidents per category/year, number of systems without implemented password policy/total n. of systems

Such evaluation metrics had been used to assess the success of the first ECSM, in 2012, as presented in the ENISA (2012) relevant report.

Guideline 5: Member State Coordinators are urged to define evaluation metrics at the design level to ensure that they collect the necessary data for assigning values to the metrics after the completion of the ECSM month events.

3.2 Evaluation Metrics

Some indicative recommended information that are important for evaluating the ECSM overall and per country:

Overall ECSM evaluation	**ECSM evaluation per country**
Communication channels used per category of recipients	Communication channels used per country
Total security themes covered per week	Security themes covered per week
Total number of security themes covered	Number of security themes covered
Total cost of ECSM per year	Cost of a country's ECSM
Total number of events per year	Events organized per country per week Number of activities/events organized per country Time to organize ECSM per country
Average duration of ECSM months	Duration of ECSM per country
Total number of locations where ECSM events were organized	Number of events' location per country
Total number of target audience categories	Number of target audience categories
Total number of attendees in ECSM events	Number of attendees per country
Total number of visitors in all ECSM websites and ECSM central website during the awareness month	Number of visitors in national ECSM website during the awareness month
Total number of individuals participating in ECSM activities (e.g., puzzle, quiz)	Number of individuals participating in ECSM activities (e.g., puzzle, quiz)
Total number of material distributed	Number of material distributed Number of posters Number of brochures

Guideline 6: Member State Coordinators are recommended to provide information from past ECSMs (2012-2016) for assessing the metrics.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

TP-06-17-473-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-246-2
DOI: 10.2824/040879