I AM CYBER SECURITY UPDATED

European Cyber Security Month

deployment report

2014

European Union Agency for Network and Information Security www.enisa.europa.eu

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.

Authors

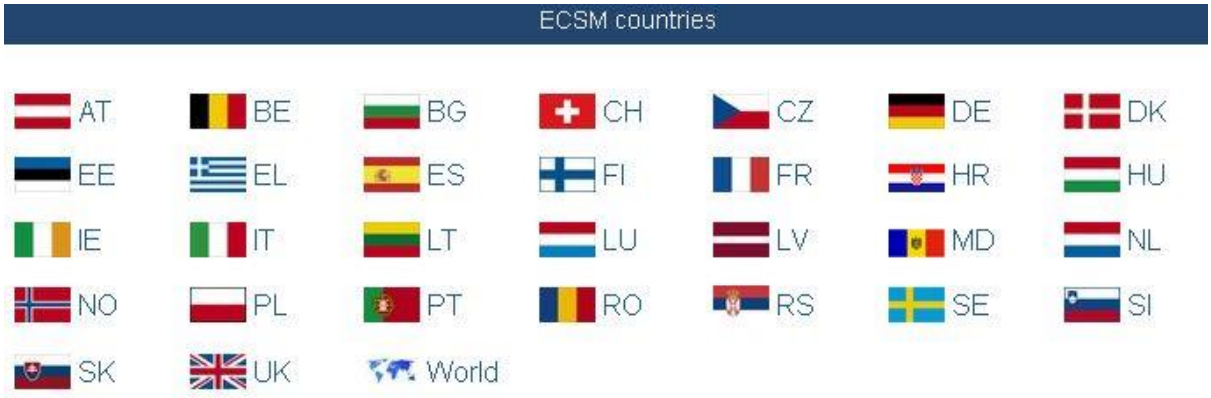
For contacting the editor please use stakeholderrelations@enisa.europa.eu ref Daria CATALUI and Demosthenes IKONOMOU.

Contact

For media enquires about this paper, please use press@enisa.europa.eu**.**

Acknowledgements

We would like to express gratitude for the work and support of Ann-Sofie RONNLUND (EC DG CONNECT). Furthermore appreciations for the work of all coordinators from the 30 ECSM countries who participated for ECSM 2014 deployment:



Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

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

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

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2014

Reproduction is authorised provided the source is acknowledged.

ISBN TP-04-14-679-EN-N 978-92-9204-092-5 10.2824/3270

Executive summary

ECSM is an EU advocacy campaign that promotes cyber security among citizens and advocates for change in the perception of cyber-threats by promoting data and information security, education, sharing of good practices and competitions.

The European Union Agency for Network and Information Security (ENISA), the European Commission DG CONNECT and Partners followed a strong partnership for the implementation of European Cyber Security Month (ECSM) in 2014.

Action! During October at the local level

In October, the community has pinpointed the following weekly Network and Information Security topics on the agenda:

- 1st week: Training employees, targeting public and private organisations
- 2nd week: PC and mobile security protection and updates, targeting all digital users;
- 3rd week: Coding, targeting students
- 4th week: Cyber security exercises, targeting technical expertise;
- 5th week: ePrivacy, targeting all digital users

With a good reach proved by online analytics, with a good participation rate evidenced by the number of countries, with a significant motivation for future edition verified by coordinators replies, we can conclude that the European Cyber Security Month 2014 edition was very successful. However much more must be done in order for EU citizens to benefit the most and we suggest recommendations in the last chapter.

Table of Contents

Executive summary iv

1 Introduction 1

2 Implementation 4

2.1 Develop a stable Model of coordination at European level and MS level 4

2.2 Enhance Content of ECSM 8

2.3 Improve International Cooperation 10

3 Evaluation 11

4 Conclusions 14

References 15

1 Introduction

ECSM is an EU advocacy campaign that promotes cyber security among citizens and advocates for change in the perception of cyber-threats by promoting data and information security, education, sharing of good practices and competitions.

The objective of this report is to:

1. Present this preparatory work;
2. Carry out an objective evaluation by setting up an external survey open to the ECSM coordinators;
3. Draw conclusions that can be used in future editions of the ECSM.

European Cyber Security Month 2014 has been designed to be an advocacy campaign focused on Member States of the EU also involving partners. The project life cycle included coordinators calls, webinars, face-to-face meetings, monthly news updates, high-level launch event, website resources, and weekly publication of materials. A short summary of the campaign includes:

- A coordinated EU campaign in the area of NIS that takes place every year in October;
- This campaign brings together Member States' (MS) activities under a common agenda. Through this mechanism ENISA seeks to promote the transfer of good practices, know-how across MSs and network between teams;
- ENISA plays the role of a facilitator or of a broker. However, the MS are responsible for their own activities as well as the macro management of the ECSM. The decision on the direction of the ECSM 2014 was taken in consultation with representatives of the Italian and Luxemburg teams as part of the macro management team motivated by their EU Presidencies (IT during October 2014, LU during October 2015);
- For this purpose an enlarged team comprised of representatives by all MS (involved in national campaigns) is formed, supported by ENISA;
- Although the ECSM only lasts for one month (as the name suggests) it requires intensive preparation in advance. There is scope in saving time after the October, to carry out the evaluation of the activities accomplished throughout October.

Some quotes

Commissioner VP Kroes' statement for the ECSM: "The Internet and its many services bring many benefits to our society: not least significant growth of our economy and millions of jobs. But we need to build and restore trust if we really want to achieve those benefits. When it comes to cyber security, it is in our common interest to be much more responsive and resilient to cyber threats. ENISA can both play an operational and a strategic role to ensure that Europe is ready for the challenge, together with public and private parties. Each one of us must play our part in the cyber-security challenge: every citizen, every business, and every government. So I hope that the European Cyber Security Month raises more awareness – let's get people talking!"

ENISA's Executive Director, Prof. Udo Helmbrecht, commented: "*The internet of things, where every electronic device will be uniquely accessible and identifiable over the internet, is approaching quickly. This has a profound impact on all aspects of citizens' everyday life, as e-services are all now totally dependent on an open, safe and secure cyberspace. These are the technologies that are being built today and that will deliver the services of the future.*

It is therefore essential for citizens to participate actively in improving information security, for ENISA to facilitate improvement processes and for Member States to ensure that security policy supports the internet based economy envisaged for Europe 2020. Year by year we have been consolidating this trust partnership for Cyber Security Month and I am honoured to see the high level of engagement from partners. On behalf of my team, thank you all! ".

Target audience

ECSM is an annual advocacy campaign that includes both the general public , acting as 'EU digital citizens' and specific groups focused on Member States stakeholders from public and private organisations e.g. IT experts, NIS authoroties, etc . The engagement model that ENISA uses is depicted in the graphic below. It represents the stakeholders that are involved in the ECSM and the way the Agency implements the brokerage role. The ECSM campaign is supported by ENISA and DG CONNECT, the main contact in member states are through the National Laison Officers- NLO[1] network, partners from public and private organisations, and networks of multipliers e.g. Europe Direct. Furthermore the composition of the NLO network includes Member States representatives - one from each EU and EEA country. A representative from the European Commission and a representative from the Council of the European Union are also part of the network. Although not formally based on the ENISA Regulation, this network is of great value to ENISA, as the NLOs serve as ENISA's important point of reference into the Member States on specific issues. ENISA also gains access to a network of national contacts through individual NLOs, reinforcing the activity of the Agency in the Member States.

Graph engagement model

Structure of this document

This document will present to the reader the organisational aspects of the ECSM 2014 putting things into perspective. We will refer to the motivation and concept behind the month, participation, and evaluation including analytics. The evaluation report from 2013 with its recommendations was taken into account and we refer to each of the recommendations giving details about the follow-up implemented in 2014.

[1] ENISA has set up this network of National Liaison Officers (NLOs).

2 Implementation

The European Cyber Security Month 2014 benefited from planning that took into consideration recommendations from the roadmap released in the previous year. In 2013, the main recommendations[2] regarding future editions of the advocacy campaign were grouped into three pillars:

Develop a stable Model of coordination at European level and MS level

- ✓ Plan in advance all steps and communicate them
- ✓ Improve content and participation
- ✓ Improve interactivity

Enhance Content of ECSM

- ✓ Continue the development of repository of materials
- ✓ Keep encouraging private-public common activities
- ✓ Introduce a best practice section on the website

Improve International Cooperation

- ✓ Exploring common webinars and e-learning solutions
- ✓ Develop an International training kit for NIS activities
- ✓ Advance planning

In the following sections we will briefly present how the lessons learned from 2013 were imlemented.

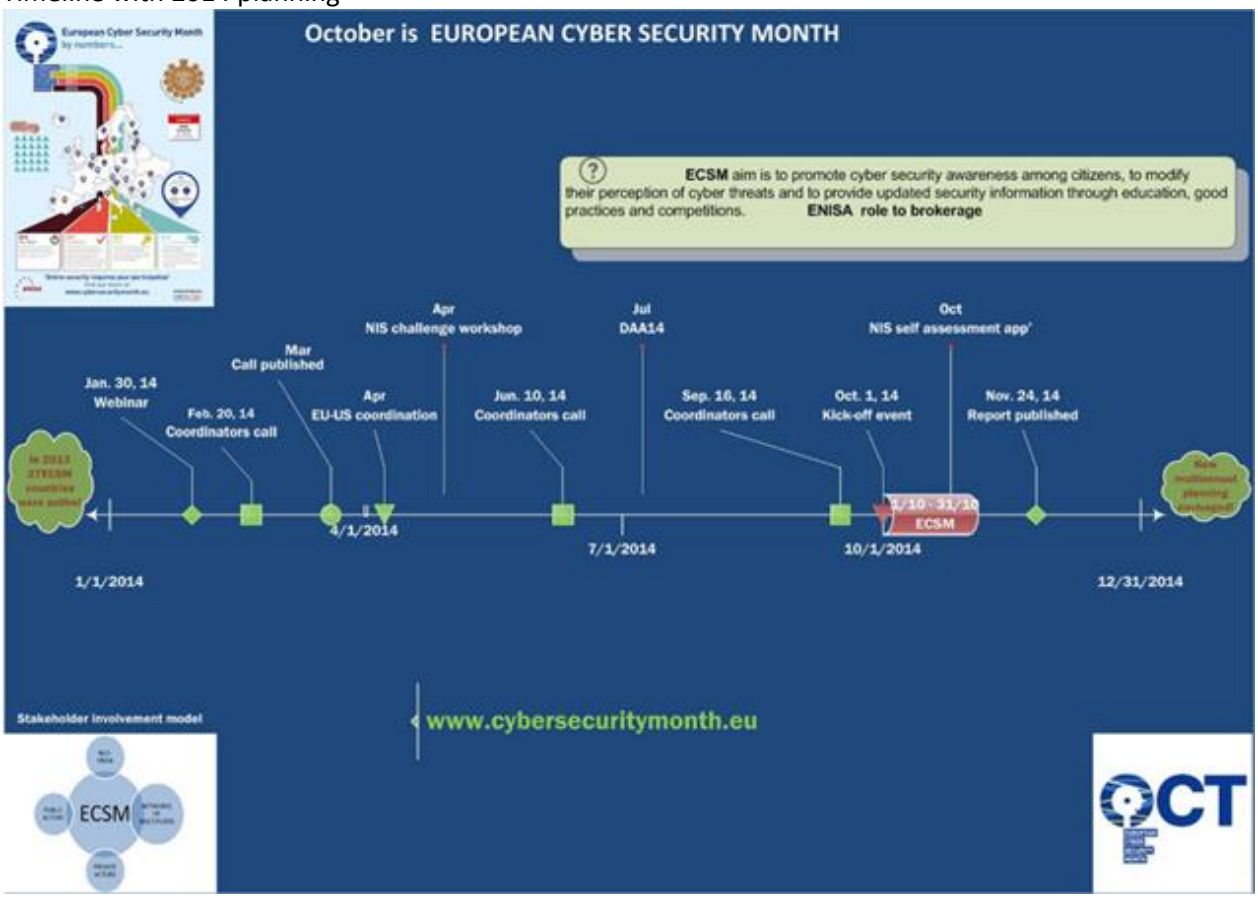
2.1 Develop a stable Model of coordination at European level and MS level

In the beginning of the year, the ECSM team[3] organized consultation meetings with the main stakeholders, e.g. NLOs, DG CONNECT, CODE Week team, US NCSM, at European level and international level and completed a detailed plan well in advance of the event. Moreover all steps were explained on many occasions and communicated to all stakeholders. The strategy was then mapped to a timeline and used in order to build coalitions and reach other actors.

More milestones were identified and more synergy actions were built with other networks. For example this timeline shows the coordination calls but it doesn't include about all the other planning steps[4] that were agreed with multipliers like Europe Direct, Code Week, Safer Internet, and US NCSM.

[2] Roadmap for ECSM, 2013 report http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2013
[3] ECSM core team consisted of: ENISA, DG CONNECT, IT and LU representatives
[4] E.g. common publication of material, international Twitter chat, etc.

Timeline with 2014 planning



Additionally in order to improve content and participation, both in terms of quality and quantity, the website www.cybersecuritymonth.eu represented the single main stop for citizens to look for information and the place for ECSM coordinators to update details about activities taking place at the local level. The site management was done by ENISA, but MSs Coordinators retained full control and responsibility for their content. Changes and updates were supported by the team.

In order to improve interactivity, the team released a Network and information Security Quiz[5] for users. The audience for this quiz was the broader public and the quiz was intended to combine an entertaining activity with a serious goal: offer an opportunity for participants to familiarise themselves with some of the key themes of NIS education and some of the ENISA recommendations, including material developed in recent years by ENISA through its work. Some questions are also directly connected to the concepts introduced in the first part of this report.

The quiz contains 10 NIS questions and in total, together with input forms, it should take approximately 10 minutes to complete. Each question starts with a short narrative and then a dilemma or a direct question. For each answer (either correct or not) there is then a short explanation/discussion with some further suggestions. A profile will be generated based on the overall result of the quiz. The profile can be one of the following:

1. Beginner: with limited number of correct answers. This profile signals limited level of skills or knowledge of NIS (according to the quiz and the difficulty level selected by the participant).

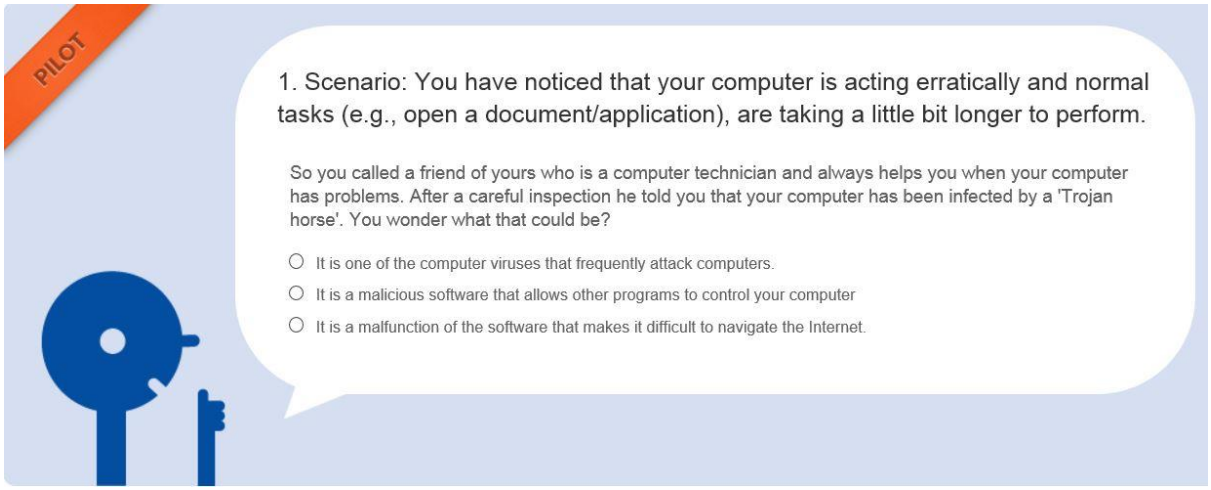
2. Intermediate: good number of correct answers. This profile has a reasonable level of skills and knowledge of NIS (according to the quiz and the difficulty level selected by the participant).

3. Advanced: high number of correct answers. This profile has an excellent level of skills and knowledge of NIS (according to quiz and the difficulty level selected by the participant).

For each generated profile further indications are offered in terms of documentation and material to consult with particular attention to ENISA reports. At the low and medium levels there is also the suggestion for attempting the next confidence level quiz.

The application is available on the website[6] from October 2014 as a pilot with a possibility of renewal after the first evaluation.

Sample question:



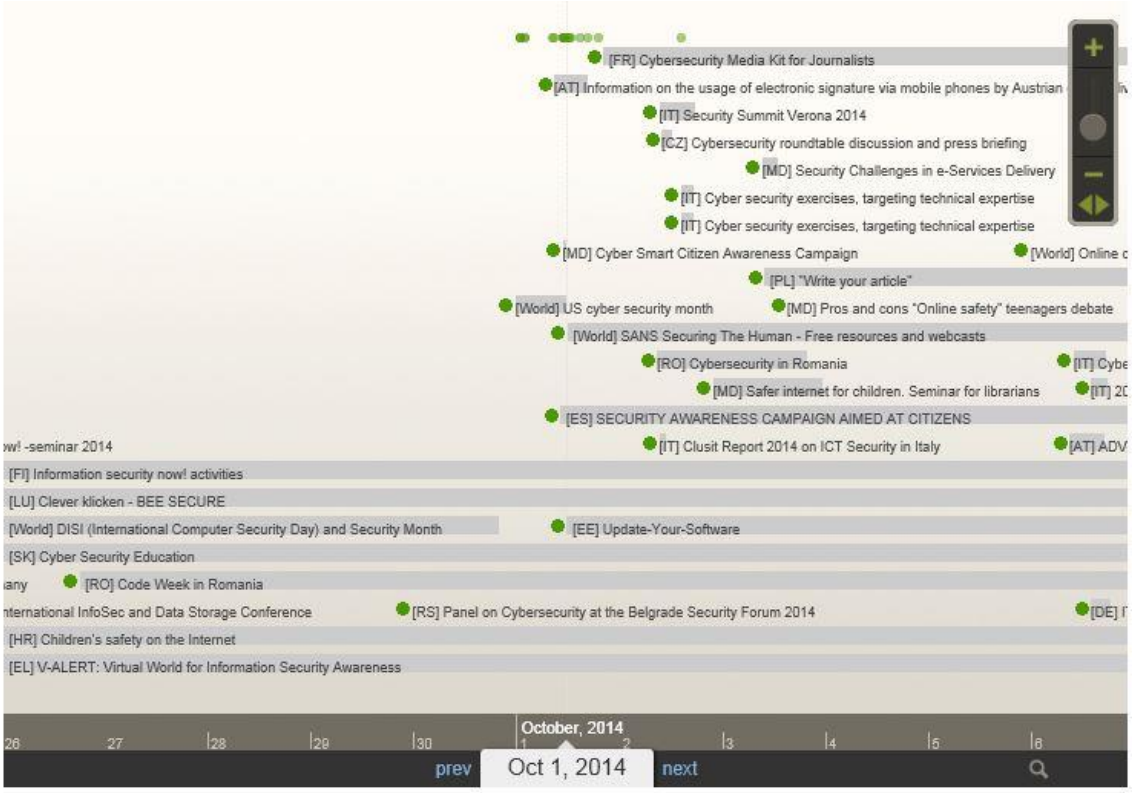
[5] Roadmap for NIS education programmes in Europe http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/roadmap-for-nis-education-programmes-in-europe
[6] Link http://cybersecuritymonth.eu/references/quiz-demonstration

2.2 Enhance Content of ECSM

The Agency coordinated the release of deliverables in alignment with the weekly topics of October. This way we continued the development of repository of materials and we participated with content for updating the skills of the users. The publication time and direct link in the table below:

CONTENT	LINK	
education map News item TITLE: October is Cyber Security Month! **Published:** http://www.enisa.europa.eu/media/news-items/october-is-cyber-security-month		
Published Materials in more EU languages Press release http://www.enisa.europa.eu/media/press-releases/countries-aligned-for-the-deployment-of-the-european-cyber-security-month Information Briefs http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2014		
Report "Public Private Partnerships in Network and Information Security Education" News item **Published**: http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/public-private-partnerships-in-network-and-information-security-education		
Universities databases News item **Published:** https://www.enisa.europa.eu/media/news-items/list-of-available-courses-in-nis-now-available		
Report "Cyber Security competitions- status in Europe" http://cybersecuritymonth.eu/cyber-security-challenge-competition		
Report "Roadmap for NIS education programmes in Europe" News item **Published**: http://www.enisa.europa.eu/media/news-items/recommending-educational-tools-and-scenarios-for-nis-education		
NIS quiz **Published:** http://cybersecuritymonth.eu/references/quiz-demonstration		
International launch of TIPS for users **Published:** **http://stopthinkconnect.org/campaigns/details/?id=442**		
Materials from Partners for ECSM community	Every Friday	Twitter

One of the approaches that was continued from the 2013 edition was keep encouraging stakeholders to participate with common private-public activities. As a result of this ECSM achieved great impact with more activities in all countries, a sample on how the calendar looked like below.



In addition, the Agency introduced a best practice section on the website. The team promoted the stories and work of champions[7] of cyber security from member states.

AT: Marion Marschalek

I personally found fascination in dissecting software. The more I dissect, the better I understand, the more I love to learn more. I think every human is naturally driven to learn, to build and to improve; but when I started this, I admit, all the binaries did not look all that appealing to me.

I had to take a second look, then a third one, understanding a bit more every time, and finally having fun dragging all my new knowledge together. And now... I do this every day, with passion.

RO: Andrei Avădănei

Challenge yourself and learn by participating to DefCamp.

UK: Chris D Doman

Without the UK's Cyber Security Challenge I probably wouldn't have found myself in such an exciting position, and campaigns such as ECSM are key to getting more people to realize how much their passions for technology are needed, both right now, and for the foreseeable future.

[7] Direct link http://cybersecuritymonth.eu/cyber-security-ambassadors

2.3 Improve International Cooperation

The ECSM team entered very early into consultation and advance planning with the counterparts from the NCSM- National Cyber Security Month US. This supported establishing good contacts and common actions between teams. Furthermore the following was achieved in collaboration:

1. Panel with representatives of NCSAM and ECSM for promoting Cyber Security Month during IGF- Internet Governance Forum 2014 Istanbul;
2. Publication of a report: "Public Private Partnerships in Network and Information Security Education"[8];

3. International Twitter chat on tips to follow for NIS security;
4. Publication of "Mobile Tips" for users, important to mention that this common actions is already at the 2nd consecutive edition[9];

5. NCSM representative in the Launch event of ECSM in Brussels.

We believe that the international cooperation has a real potential to grow, however a multi annual planning with clear milestones is currently missing and it should be agreed in advance.

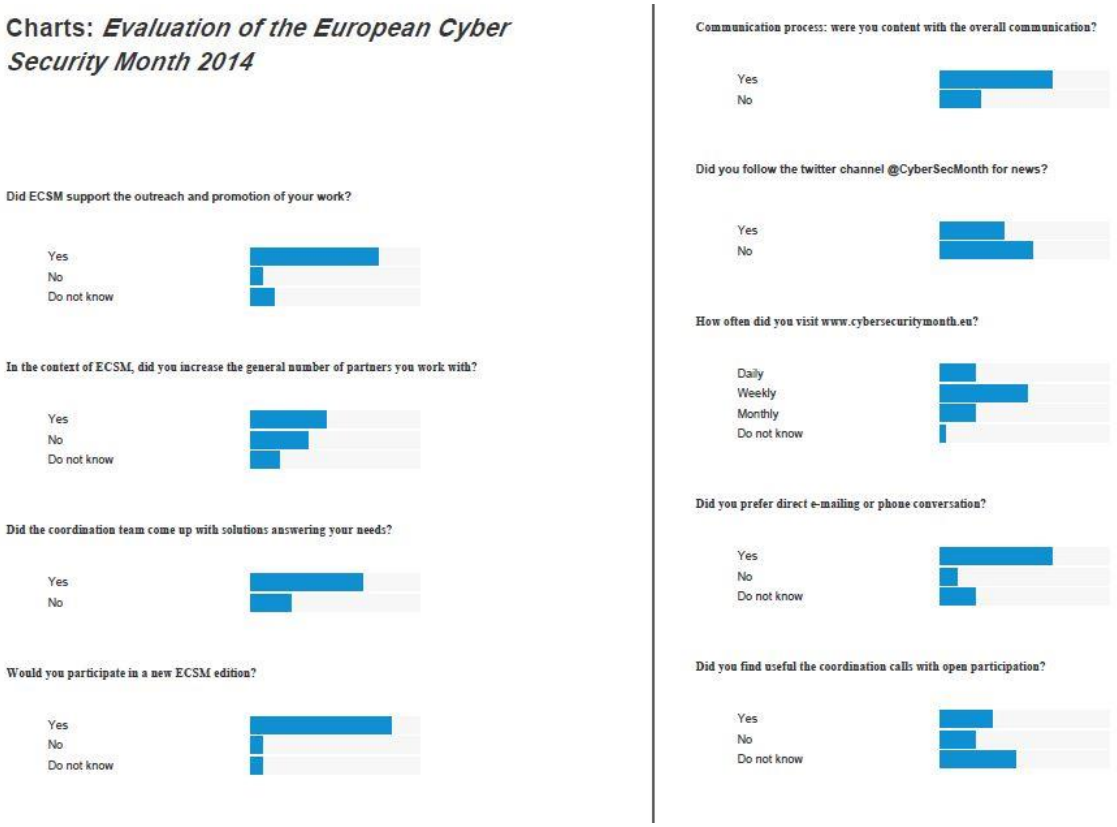
[8] http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/public-private-partnerships-in-network-and-information-security-education
[9] http://stopthinkconnect.org/campaigns/details/?id=442

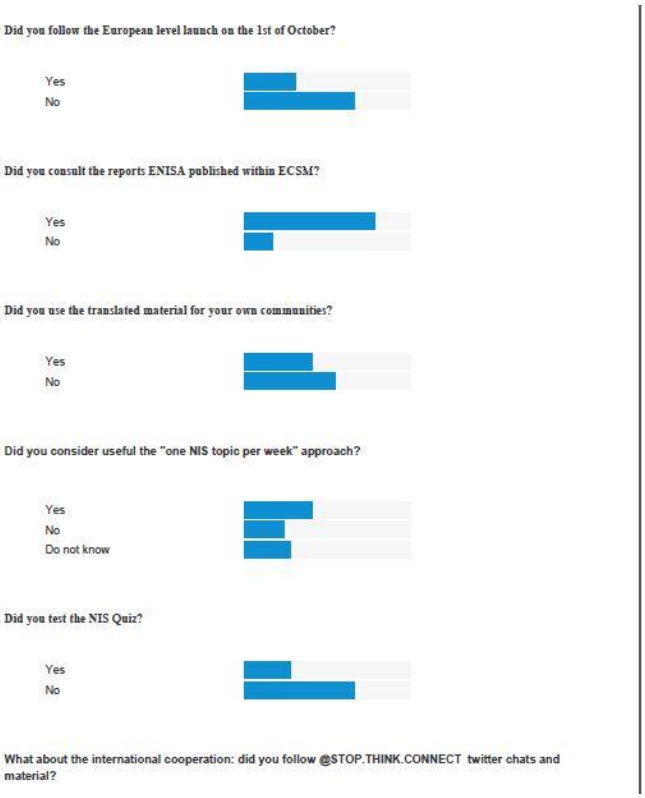
3 Evaluation

The direct beneficiaries of the results of this work are the EU citizens, targeted by different categories, as well as end user organisations from public and private sectors (in particular in the area of EU NIS education). These stakeholders were expected to reap the following benefits:

- Develop knowledge and corresponding ICT skills by being part of a best practice sharing community;
- Improve and enhance contacts with stakeholders of similar interests and profiles.
- Increase citizens' awareness and governance on privacy when using online tools.

Coordinators in the Member States played a central role in achieving these benefits. This is why in order to evaluate this edition of the campaign we set up a survey and asked a number of questions to get their feedback. The survey was closed and focused on the coordinators involved in the campaign. The charts below present their replies, 29 participants in total. In comparison to previous editions we improved the phase of the evaluation taken into account larger consultation in order to avoid biases and integrate more opinions in the future planning of ECSM.





Furthermore the replies from the charts of the evaluation of European Cyber Security Month 2014 clearly show that:

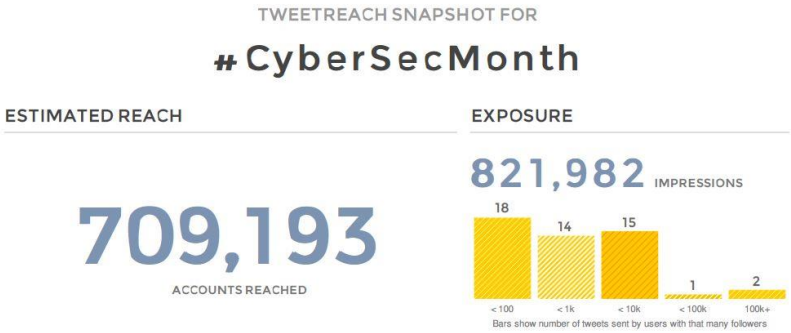
- Several communication channels have to be used and Twitter cannot be used exclusively, we may further use coordination calls, meetings, newsletters;
- The coordination team responded to the needs of the coordinators;
- ECSM brings added value and there is a clear statement of continuation;
- ENISA reports and material are used by the community;
- More effort has to be put in communicating all the material produced by ENISA and MSs.

These early conclusions will be complemented at a later stage by qualitative information (e.g. assessment of the NIS Quiz through focus group) and used for the planning and deployment for next editions.

It is presented below some other graphs regarding the use of the website, twitter reach and map with geographical spread of the activities.

- Website sessions during the period end September to end October

- Twitter performance



- Media reach

There was increased online and social media presence on 1 October to coincide with the start of **European Cyber Security Month**. With over **300 Tweets** and **70 Facebook** mentions, there were also over **40,000,000 online users** reached by articles mentioning ENISA.

- Comparison 2013 vs 2014 in numbers:
  - Countries involved 2013: 27, **2014:30**;
  - Twitter followers 2013: 964; **2014: 2223**;
  - Kick off participation 2013: approx. 100 in total; **2014: approx. 200**;
  - Materials published 2013: 2; 2014: 5 general and 2 tools e.g. NIS universities map and NIS quiz;
  - Activities taken place: 2013: 115 vs **2014: more than 184** [some countries like NO and SE encoded one general entry for tens of local activities; e.g. in annex CZ example in infographics].

The annual editions of ECSM improve each year the beneficiaries reach, e.g. 2014 vs 2013. However more could be done if more partners would join and participate according to the engagement model e.g. public- private partnerships.

4 Conclusions

The Agency will continue to support the European Cyber Security Month, but will aim to continually increase, according to the work programme 2015-2016, the involvement of Member States in the coordination and deployment.

We call on Member States to promote and inform their NIS stakeholders on time!

We call on the European Commission to further provision on translations and support the coordinators!

In recent years, the European Cyber Security Month has expanded its outreach with numerous activities in the Member States, reaching a large number of European citizens. In 2015 and 2016 the work programme[10] mentions the ECSM will be further developed following its basic principles, namely:

- Support the multi-stakeholder governance approach.
- Encourage common public-private activities.
- Assess the impact of activities, optimising and adapting to new challenges.

Moreover Member States are encouraged to develop ownership of the campaign and support:

Building together a joint EU advocacy campaign on NIS topics!

[10] http://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programmes-general-reports

References

ENISA

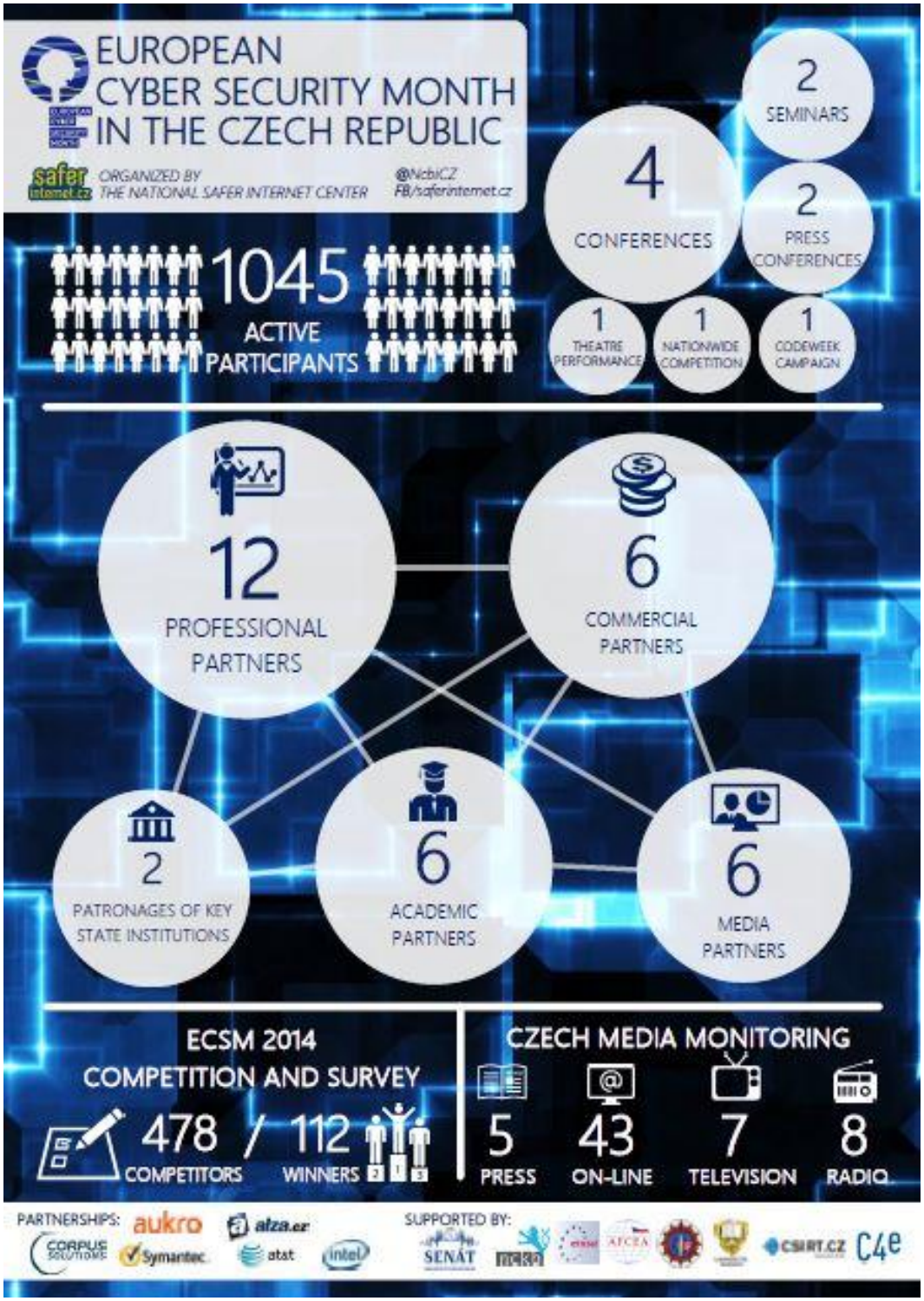
[1] www.cybersecuritymonth.eu

[2] www.enisa.europa.eu

[3] "An Open, Safe and Secure Cyberspace" EU Cyber Security Strategy http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

[4] ENISA Work Programme 2015 http://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programmes-general-reports

Annex A: An infographic from MSs: CZ ECSM in numbers



ISBN TP-04-14-679-EN-N 978-92-9204-092-5 10.2824/3270

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 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

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