Udo Helmbrecht, Executive Director, ENISA

Speech at the Committee on the Internal Market and Consumer Protection

IMCO, EUROPEAN PARLIAMENT
23 JUNE 2015

Dear Ms Vicky Ford, members of the IMCO committee and representatives of other institutions present

I would like to thank you for the opportunity to address you here today and to provide you with an overview of how ENISA (European Union Agency for Network and Information Security) is contributing to a high level of network and information security within the European Union and in order to raise awareness in network and information security.

I will also provide you with an overview on how the Agency supports the development of culture of network and information security for Europe as a whole and especially its citizens.

Allow me to start with what it is that ENISA does. The Agency is a centre of expertise for cyber security in Europe. The Agency works closely together **with public sector,** represented by Member States, the European Parliament, the European Commission, **and private sector**, to deliver advice and solutions that are based on experience. This includes, the pan-European **Cyber Security Exercises**, the development of **National Cyber Security Strategies,** Computer Emergency Response Teams **(CERTs) cooperation and capacity building**, but also studies on **secure Cloud adoption**, addressing **privacy and data protection issues**, **eIDs and trust services**, and identifying the **cyber threat landscape**.

ENISA supports the European Union (EU) and the Member States in enhancing and **strengthening their capability and preparedness to prevent, detect and respond to network and information security issues.** ENISA also supports the development of the EU **policy development** on matters relating to network and information security, thereby contributing to economic growth in Europe's internal market.

ENISA works towards the creation of an effective culture of Network & Information Security (NIS) throughout the EU, in a cross-border and cross-community environment and regular interaction.

In addition, ENISA carries out tasks conferred on it by legal acts of the Union (for example, Article 13a of the Directive 2002/21/EC (amended by Directive 2009/140/EC); Article 19 of the Regulation 940/2014, etc.).

By doing this, the Agency aims at creating **communities and synergies** in areas such as **finance, critical infrastructure, telecommunications, cloud computing, health**, and others to contribute to a high level of network and information security in EU.

Strategic information on cybersecurity which is designed to assist for the policy makers is made available through specialised reports (e.g. the **ENISA Threat Landscape**[1]) and web services (e.g. the web summary of **National Cyber Security Strategies**).

I am proud to note that ENISA's contributions promotes best practices in network and information security and that understanding of the **cyber dynamics. Its recommendations** are an important tool towards an **active and agile security management.**

The importance of raising awareness

As a part of its yearly activities, ENISA actively contributes to the joint activity with the European Commission DG CONNECT, known as **the European Cyber Security Month (ECSM)**[2]**.** The ECSM is an **EU advocacy**

[1] https://www.enisa.europa.eu/media/press-releases/enisa-draws-the-cyber-threat-landscape-2014

[2] https://cybersecuritymonth.eu/

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.

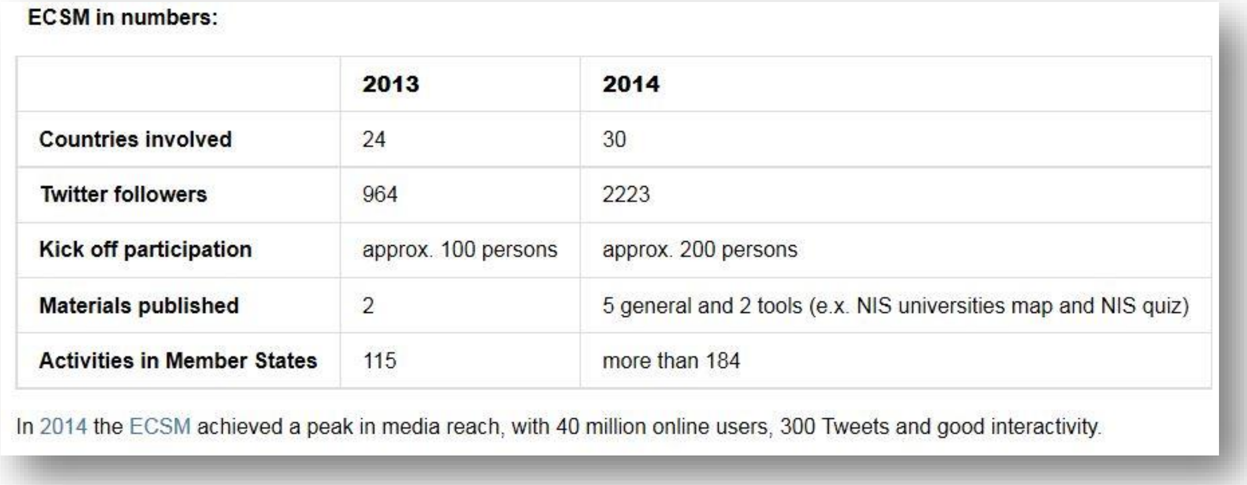
Under this initiative different activities take place all over Europe, while providing material online through ENISA's website, including **7 Information Briefs with recommendations on cyber security topics in the EU languages.**

The recommendations include:

- Advice on network and information security for educators and employees,
- The risks associated with the use of discontinued software or anti-malware,
- Online data protection rights, and understanding lessons learned.

Lessons learnt

A report on the deployment of the European Cyber Security Month presents its preparatory work, gives an objective evaluation, and draws upon the conclusions that can be used in future editions of the ECSM. In numbers, we witness an increase in the countries involved and the number of online followers via the social media (twitter). In particular, in 2014[3] the ECSM[4] achieved a peak in media reach, with 40 million online users, 300 Tweets and good interactivity. Furthermore, more activities and related material has been generated, while participants at kick-off have doubled.



ECSM in numbers:

	2013	2014
Countries involved	24	30
Twitter followers	964	2223
Kick off participation	approx. 100 persons	approx. 200 persons
Materials published	2	5 general and 2 tools (e.x. NIS universities map and NIS quiz)
Activities in Member States	115	more than 184

In 2014 the ECSM achieved a peak in media reach, with 40 million online users, 300 Tweets and good interactivity.

Based on previous experience from the Cyber Security Month (2013 and 2014) conclusions and recommendations are focused on three pillars:

- Develop a model of coordination at European level and Member State (MS) level;
- Enhance the content of ECSM by continued development of repository of materials. This is important for establishing dialogue channels between MS;

[3] https://www.enisa.europa.eu/media/press-releases/countries-aligned-for-the-deployment-of-the-european-cyber-security-month

[4] https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign

- Improve international cooperation by exploring common webinars and e-learning solutions and develop an International training kit for NIS activities.

Online privacy tools for the general public

ENISA is currently developing a tool with online privacy tools for the general public.

This is a recently started activity which aims to increase assurance in the field of online privacy tools. In 2015 ENISA will perform a feasibility study on the creation of a portal that will provide information to citizens on the use of online tools that enhance privacy.

As the outcome of this activity, a portal on trustworthy privacy tools for the general public will be created. This portal will provide tools that:

- Have been evaluated by privacy experts;
- Easy to understand and use by the average user;
- Kept up-to-date with latest information;
- Are supported by the EU privacy community.

In addition, its extensive collection of **awareness material**[5] is promoted on every opportunity such as during the celebration of the Europe Day and the activities organised in cooperation with local communities. For example, **ENISA staff members visited schools in Agency's host country Greece** for a "Back to school" session, giving the opportunity to students to learn more about the Agency's work in cyber security for Europe. Students had the chance to get informed about staying safe online and online hazards such as cyber-bullying, while having the opportunity to discuss and share experiences from their perspective on the use of online media.

Challenges for the future

Various recent studies, including those of ENISA, demonstrate that the threat landscape will get worse, unless we take firm action. It is expected there will be a significant evolution in the top threats, with new, more sophisticated malicious attacks on critical services and infrastructures, with a dramatic increase in data and security breaches (25% increase over the same period last year).

ENISA's experience and expertise are here to offer the Agency's and its staff support to citizens by using its stakeholders from Member States and private communities **to provide outreach**.

The European Commission recently published Digital Agenda Scoreboard. It shows that almost 75% individuals in Europe Union use internet on a regular basis[6]. One should understand that any **individual one of these connections is capable of attacking a banking system to extract funds unlawfully, attacking a critical infrastructure that controls energy, water or industrial processes or assuming the electronic identity of another individual.** All this is possible from any internet connection in the world.

[5] https://www.enisa.europa.eu/media/news-items/8th-may-celebrating-europe-day-with-enisa

[6] http://ec.europa.eu/digital-agenda/en/digital-agenda-scoreboard

ENISA plays a critical role in helping EU Member States and European industry to develop their capabilities and expertise to be able to respond to increasing cyber security threats and challenges of both today and tomorrow.

In order to address this increasing political and economic challenge, **the Agency's capacity is limited.** It needs to be provided with additional human and financial resources to address the tasks assigned to it and to successfully deliver tangible results.

The 2013 Regulation of ENISA along with the new legislative initiatives increased the scope of tasks being required of ENISA. ENISA is in an increasingly difficult position to keep on delivering.

Concluding remarks

- ENISA's size necessitates to place its focus to the public and industry sectors with efforts made to increase outreach to citizens.
- Public and private bodies need to get involved in cybersecurity education and Public-private partnerships.
- ENISA's Work programme, although may seem specialised at a first glance, in essence it provides access to the information needed for public and industry to be part of the online society and gain from the benefits within the Digital Single market.
- In reality our studies have one inherit attribute. These studies are addressed to targeted audiences, which make it easier to segment and address their special needs and requirements.
- ENISA when implementing its mandate, is raising awareness in network and information security, which constitutes a horizontal action and integral part of every deliverable.

To conclude, ENISA is here to address the cyber challenges in Europe that we are facing. Although the Agency is delivering in an efficient manner, further investments in the Agency in terms of financial and human resources will enhance Europe's political aspirations to contribute to a high level of cyber security across the EU and to pave the way for a safer and resilient Europe.

Thank you very much for you attention!

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