ECSM Guidelines for Organizations

1 Background Information

European Cyber Security Month (ECSM) is an EU awareness campaign that promotes cyber security among citizens and organizations about the importance of information security and highlighting the simple steps that can be taken to protect their data, whether personal, financial and/or professional. The main goal being to raise awareness, change behaviour and provide resources to all about how to protect themselves online. 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 organizations on the design and implementation of European Cyber Security Month awareness campaigns, though a set of 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 ECSM Events/Material

2.1 Setting the Objective for Information Security Awareness

To develop an effective information security awareness event/material within the scope of ECSM, organizations should develop a concise understanding of security awareness and what they aim to achieve. For this purpose, this document presentfs widely accepted definitions of information security awareness.

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.

Information security awareness is most known wihtin organizational context, where organisations implement security awareness programmes, so that employees develop the necessary knowledge and skills for protecting organisational assets from cyber threats, develop appropriate security behaviour and cultivate an information security culture towards protecting information systems. 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). Information security awareness in organizations has been also 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).

Therefore, different types of awareness strategies can be developed, including various delivery channels. Security awareness events/materials that can be considered for registration at ECSM may include conferences, seminars, workshops, online games, posters, and others (please see a list of delivery channels at ENISA (2011)). It is important to recognize that the path towards more secure users' behavior in organizations starts with security awareness, but ultimately leads to the development of an organizational cyber security culture. Developing cyber security culture differs from security awareness; organizations start with information security awareness aiming to attract users' attention to security, however ideally they need to develop an organizational cyber security culture which involves changing users' basic beliefs, priorities and values that drive their actions and decision making.

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 organizations aiming to implement 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 organizations implementing ECSM campaigns.

Guideline 1: Organizations are encouraged to create campaigns aiming at activating users to protect information from security threats. Campaigns are expected to attract recipients' attention, make them recognize information security concerns and respond accordingly. Developing an organizational cyber security culture starts with security awareness programmes. Awareness 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 an information security awareness campaign within ECSM requires proper formulation of a project plan, including specifying the implementation team, their roles and responsibilities, the budget, awareness activities, milestones, timeline and deadlines.

When specifying the budget, organizations should consider personnel costs, operational costs, advertisement costs, any technical development and support costs. For internal purposes, it is important to produce a documentation of the overall project plan. The documented project plan will support the implementation of the campaign and can help the organization to assess and guide future initiatives, given that ECSM is a yearly initiative.

Guideline 2: Organizations are recommended to develop an awareness campaign 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

It is imperative to define the target group or groups of a security awareness event/material in the early stages of planning (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 overlap 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 organizations, 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

Table 1 Categorization of Awareness Target Groups (ENISA, 2010)

An obvious target for organizations is internal users and business partner users; i.e., business users. However, organizations are also encouraged to plan awareness events within ECSM that will target general users or young people. General users and young people may potentially be customers of the organization's online services or software. A local National coordinator can guide the organization for the appropriate timing and location of the event, so as to fit the overall ECSM and maximize visibility and participation. For business users the organizations may consider separating the target audience into groups based on their organizational role.

CATEGORIES OF BUSINESS INTERNAL USERS	SOURCE
Based on their organizational role: a) Employees b) Mid-level managers c) Executive management d) System Administrator	ENISA (2010)
Based on their organizational role: a) Executive Management b) Security Personnel c) System Owners d) System Administrators and IT Support Personnel e) Operational Managers and System Users	NIST (2003)
Based on other criteria: a) Current level of computer usage b) What the audience really wants to learn c) How receptive the audience is to the security programme d) How to gain acceptance e) Who might be a possible ally	Peltier (2005)
Based on other criteria: a) Cultural biases b) Risk perceptions and misperceptions	Tsohou et al. (2005)

Table 2 Indicative Target Groups for Business Internal Users

Guideline 3: Organizations need to clearly define the target group or groups of their campaigns. Organizations can broadly separate target audience into general users, young people or business users. The design of the awareness events should be customized upon the defined target groups. For business internal users organizations can separate groups based on organizational role, and other criteria.

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, within the scope of the target audience
- 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; ENISA, 2011; 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.

Organizations 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 (ENISA, 2011, p.35). Another option for organizations 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 4: Organizations 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 awareness campaign planning. 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. Organizations are encouraged to study the recent landscape of security and privacy threats, before deciding the themes of their ECSM 2017 event. For example, ENISA (2017) has identified current top cybersecurity threats. 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). Organizations are encouraged to consider the following themes that will feature ECSM 2017: Workplace Security (e.g., malware, Ransomware, phishing, etc.), Governance & Privacy Challenges (e.g., GDPR, NIS Directive, e-privacy regulation, etc.), Home Security (e.g., IoT, home network security, online fraud, online user privacy, etc.), and Cyber Security Skills (e.g., education, skills, certifications, etc.).

Guideline 5: Organizations 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. Organizations may decide the best timing and location of their planned events, in collaboration with their ECSM local National Coordinator.

3 Guidelines for Aligning Awareness Events/Material with ECSM

3.1 Creating Public-Private Partnership for ECSM campaigns

ECSM encourages public–private partnerships and it would be beneficial for organizations to develop security awareness events in collaboration with their local ECSM national coordinator. Organizations are encouraged to complete the 'Private partnership activities template' and submit it to ENISA and/or the local ECSM national coordinator. ECSM national coordinators set the national objectives for the awareness campaigns. Private and industrial organizations have own objectives for their planned awareness events. The 'Private partnership activities template' will assist communicating

Guideline 6: Organizations that are interested in ECSM public/private partnership are encouraged to complete and submit the 'Private partnership activities template'.

3.2 Establishment of Awareness Event/Material within ECSM

Organizations that want to register an event at ECSM are encouraged to follow the new procedure described in the ECSM website (https://cybersecuritymonth.eu/new-event). The procedure to register an event is simple and aims to ensure that ECSM registered events are indeed within the scope of ECSM and in line with the applicable conditions (e.g., use of ECSM logo for the awareness event).

Guideline 7: Organizations are encouraged to register their event in the ECSM website, after submitting the relevant information through the website.

4 Guidelines for evaluating Information Security Awareness

4.1 Evaluation Approaches & Metrics

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

Table 3 Layered Evaluation Metrics (ENISA, 2010)

Some indicative recommended information that are important for evaluating an information security awareness campaign or event:

INDICATIVE SECURITY AWARENESS EVALUATION METRICS
Total number of communication channels used
Total security themes covered
Total number of security themes covered
Total cost of awareness per event
Total number of languages supported
Total number of target audience categories
Total number of attendees in awareness events
Total number of material distributed
Total number of individuals participating in awareness activities (e.g., puzzle, quiz)
% employees understanding their role in achieving security goals
Mean time between discovery and notification of a new threat
Number of security incidents due to human behavior per year
Cost of security incidents due to human behavior per year

Table 4 Indicative Awareness Programme Evaluation Metrics

Guideline 8: Organizations are urged to define evaluation metrics at the planning stage to ensure that they collect the necessary data for assigning values to the metrics after the implementation of the awareness events.

5 References

ENISA (2012), Be aware, be secure - Synthesis of The Results of the First European Cyber Security Month, Available online at: https://www.enisa.europa.eu/publications/ecsm-results

Kruger, H.A. and Kearney, W.D., (2006) A prototype for assessing information security awareness, Computers & Security, 25, pp. 289-296

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q), Computers & Security, 42, pp. 165-176

Albrechtsen, E. (2007) “A qualitative study of users' view on information security”, Computers & Security, 26(4), pp. 276–289

Albrechtsen, E. and Hovden J. (2010), "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", Computers & Security, 29 (4), pp. 432–445

Bergmann, M. (2009) "Testing Privacy Awareness", In the Future of Identity in the Information Society, IFIP Advances in Information and Communication Technology, Vol. 298, Springer Berlin Heidelberg, p. 23

Brecht, F., Fabian, B., Kunz, S., and Müller, S. (2012) "Communication Anonymizers: Personality, Internet Privacy Literacy and Their Influence on Technology Acceptance" In Proceedings in the European Conference on Information Systems 214, (2012), pp. 1–13.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", Management Information Systems Quarterly, Vol. 34, No. 3, pp. 523-548

Cetto A., Netter M., Pernul G., Richthammer C., Riesner M., Roth C., Sänger J. (2014) "Friend Inspector: A Serious Game to Enhance Privacy Awareness in Social Networks", In Proceedings of the 2nd International Workshop on Intelligent Digital Games for Empowerment and Inclusion (IDGEI), February 2014, Haifa, Israel

Cone B. D., Irvine, C. E., Thompson, M. F., Nguyen, T. D. (2007) "A video game for cyber security training and awareness", Computers & Security, 26 (1), p. 63–72

ENISA (2010), "The new users' guide: How to raise information security awareness", Available online at: http://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide

ENISA (2011), "European Month of Network and Information Security for All – A feasibility study", Available online at: https://www.enisa.europa.eu/publications/europeansecuritymonth

Haeussinger F. And Kranz J. (2013), Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior, In Proceedings of the International Conference on Information Systems ICIS 2013, Milan, Italy.

Kuo, K. and Talley, P.C. (2014), "An Empirical Investigation of the Privacy Concerns of Social Network Site Users in Taiwan", Computing and Information Technology, 5, 2 (2014), pp. 1–19.

Maeyer, D. D. (2007) "Setting up an Effective Information Security Awareness Program", In Proceedings of the Securing Electronic Business Processes Highlights of the Information Security Solutions Europe/SECURE 2007 Conference (part 1), Vieweg, pp. 49-58, 2007

Malandrino D., Petta A., Scarano V., (2013) "Privacy Awareness about information Leakage: Who knows what about me?", in Proceedings of Workshop on Privacy in the Electronic Society in Berlin, Germany, 2013, ACM, New York, USA pp. 279-284.

Moey, L. K., Katuk, N. and Omar, H. (2016) "Social login privacy alert: Does it improve privacy awareness of facebook users?", In Proceedings of the IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), May 2016.

NIST SP 800-50 (2003), "Building an information technology security awareness program, Available online at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

Okenyi, P. O., and Owens, T. J. (2007) “On the Anatomy of Human Hacking”, Information Systems Security, 16 (6), pp. 302-314

Pötzsch, S. (2009) “Privacy awareness: A means to solve the privacy paradox?”, In The Future of Identity in the Information Society (pp. 226-236). Springer Berlin Heidelberg, p.228

PwC (2016), “Insights from The Global State of Information Security Survey”, Available online at: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

Sohoraye, M., Gooria, V. Nundoo-Ghoorah, S. and Koonjal, P. (2015), “Do you know Big Brother is watching you on Facebook? A study of the level of awareness of privacy and security issues among a selected sample of Facebook users in Mauritius”, In Proceedings of the International Conference on Computing, Communication and Security (ICCCS), January 2015.

Talib, Y. A. and Dhillon, G. (2015), “Employee ISP Compliance Intentions: An Empirical Test of Empowerment”, In Proceedings of the 2015 International Conference on Information Systems, Fort Worth, Texas

Thomson, M.E. and von Solms, R. (1998), “Information security awareness: educating your users effectively”, Information Management & Computer Security, 6(4), pp. 167-173

Tsohou, A., Karyda M. and Kokolakis, S. (2015), Analyzing the role of cognitive and cultural biases in the internalization of information security policies, Computers & Security, 52 (3), pp. 128-141

Unesco (2012), Global survey on Internet privacy and Freedom of expression, Available online at: unesdoc.unesco.org/images/0021/002182/218273e.pdf

Yang X., Yue W.T. and Sia C.L. (2011), “A Cross-Culturl Study of the Effects of STEA Programs and Task Characteristics on Employees’ Behavior toward Information System Security Policy Compliance”, In Proceedings of the 6th Mediterranean Conference on Information Systems 2011, Limassol, Cyprus