Information Technology Safety Awareness – a review of regularly used terms and methods

Anikó Szarvák
Applied Mathematics and Applied Informatics Doctoral school
University of Óbuda
Budapest, Hungary
aniko.szarvak@nik.uni-obuda.hu

Valéria Póser
Applied Mathematics and Applied Informatics Doctoral school
University of Óbuda
Budapest, Hungary
poser.valeria@nik.uni-obuda.hu

***Abstract*— Over the last twenty years there have been enormous advances in the field of Information Technology. There is a quite well-defined need on information security and of course awareness. Problems with human behavior in an information security context are assumed to be caused by a lack of facts available to the audience. Awareness therefore is largely treated as the broadcast of facts to an audience in the hope that behavior improves.**

This study targets three different but connecting topics. First, reviews, the definition of Awareness and based on it creates an overview of different definitions. Second, reviews the information security awareness training, pitfalls and outcomes. And last but not least gives a non-technical way to reach people (end-users) and gives possible ways to change their behavior according to information security related topics. (*Abstract*)

Keywords—awareness, awareness training, information security awareness, information security, computer systems (*key words****)***

I. INTRODUCTION

There are a lot of available material about information security awareness, but these materials are not easy to adopt by organizations and not really known by individuals. Due the recent changes, employees are working from home instead of office, there are lot more threat appears which are cannot handle in usual information security countermeasures.

There are studies pointing out the lack of information security education, training, the awareness, consciousness itself. "An employee's perceived fairness of the ISP has a direct impact on her attitude and in turn intention toward compliance." "ISA plays a key role in employees' compliance behavior". [1]

"The proliferation of terms to describe similar concepts is identified as a big challenge for information security research. For example, information security education (ISE), information security training (IST) and information security awareness (ISA) have been defined differently by several researchers around the world, each with a different focus and purpose." [2] which is not helps the security personnel.

Decker [3] displays the lack of correlation between ISA, ISE and IST as a result of unclear definitions for the three concepts. To find the root cause of the problem, the first thing is a definition overview. There are a lot of definition on Awareness, specially Information Security Awareness.

II. DEFINITION REVIEW

Dictionary definition of awareness: knowledge or perception of a situation or fact. Knowledge that something exists or understanding of a situation or subject at the present time based on information or experience [4]. This can help to determine the definition and add a subject of the awareness.

TABLE I. AWARENESS RELATED ABBREVATIONS

Abbreviations	Expositions, Terms
	Used in this study
IT	Information Technology
ICT	Information and Communication Technology
ISA	Information Security Awareness
GISA	General Information Security Awareness
ISP	Information Security Policy
SAT	Security Awareness Training
SETA	Security Education, Training and Awareness

[a.] Table 1.Awareness related abbreviations)

We assume there are a general common understanding on we need awareness while users are enabled to use information technology both at work and at home. Reviewing the definitions, it is not easy to point out which awareness, education or training people need.

A. Definition of awareness

From different point of view, Security Awareness is defined differently, described with additional significant content. Wolf et al says "Security awareness is the effort to impart knowledge of or about factors in information security to the degree that it influences users' behavior to conform to policy" [4].

Security awareness is defined in NIST Special Publication 800-16 [5] as follows: "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly" Based on this definition Security Awareness is to recognize and to respond an event in the field of information security.

Siponen's definition on Security awareness: Security awareness is a state in which users in an organization are aware of and are ideally committed to the security objectives of their organizations. [6]

According to Information Security Forum (ISF) [7], "security awareness is a continual process of learning by which, trainees realize the importance of information security issues, the security level required by the organization, and individuals' security duties"

B. Information security awareness

Information Security Awareness: "ISA is an employee's general knowledge about information security and his cognizance of the ISP of his organization" [8] In this definition ISP is the Information Security Policy. In general, if we view the topic of information security awareness from a more nature way, we have to have a statement that there is no information security policy for general internet home usage.

Connecting to this topic, a more proper definition is added by Siponen: "ISP Awareness is defined as an employee's knowledge and understanding of the requirements prescribed in his organization's ISP and the aims of those requirements" [6]

Information security awareness can be defined as the combination of a person's knowledge of security concepts and the person's awareness or consciousness of the existence of any security related policies. [9]. According to the review of these publications we see this definition is the must proper.

C. General Information Security Awareness

Based on the statement of Information security awareness, General Information Security Awareness, hereinafter GISA, should be the definition of information security awareness for general users, but Bulgurcu et al.'s definition not reflects it. They define "General Information Security Awareness is an employee's overall knowledge and understanding of potential information-security-related issues and their ramifications, and what needs to be done in order to deal with security-related issues" [1].

D. Technology awareness

Additionally, we found a different approach of the awareness definition which comes from the technology perspective. Technology awareness as a "user's raised consciousness of and interest in knowing about technological issues and strategies to deal with them" [10].

E. Definition of information security awareness

"Security awareness contains two equally important pieces. The first piece is the dissemination of accurate, current and appropriate knowledge of policy to individuals. Policies explain to individuals the threats they need to be cognizant of as well as the appropriate actions to take upon encountering a threat. The second portion of awareness is the delivery of policy in a manner that convinces an individual to change his or her behavior. These two portions are equally important; without one, the other is ineffective." [4]

In Al-Daeef et al's review of these definition says the following: "Previous definitions have highlighted three key components of security awareness, they are; ongoing or continual process, knowledge delivery method, and individuals' behavior impact. Based on that, information security awareness has defined as the security knowledge that has been gradually acquired through a continuous and updated catchy training manner to influence trainees' behavior." [12]. We agree with this conclusion of their study. they defined the security awareness as a independent concept from ISP.

Information security awareness – ISA – knowledge, desired behavior is based on the Information security Policy – ISP – which is designed and shaped for an organization. It may contain general information and widely accepted and implemented desired behavior items, but it is consistently fitted for the organization. For example, if an organization not allows using for users / employees their own equipment for work, BYOD – and its security countermeasures – is not described in it.

Bulgurcu et al. come to the conclusion in theirs study that "ISP awareness can be different from general ISA" [1] which opens the possibility that there have to be a good definition which is able to define the information security awareness properly and independently.

Taken into consideration that every definition above is defines a piece of Awareness related to information security, information security policy, general information security we suggest splitting these into two separate definitions. One is related to compliance of an organizations' ISP and one is general, which is not related to organizations, policies. This is close to the dictionary version of Awareness, in general and relates to information technology safety.

An independent definition of Information Technology Safety Awareness is knowledge or perception of a situation or a fact in Information Technology field or related area. Based on this definition, awareness is independent from any information security policy but relying to information technology. In this definition information technology (IT) is the use of computers to store, retrieve, transmit, and manipulate data [13] or information. IT is a subset of information and communications technology (ICT). IT is including, but not limited to personal computers, mobile handheld devices, tablets, wearables and servers.

With this definition we are able to separate and distinguish a general knowledgebase from a highly shaped Information Security Policy and its expectations. Narrowing the knowledgebase, we can implement an education model, qualitative and quantitative measurement model and we are able to specify trainings to enhance the education.

F. Definition of security education security training

Security training in addition, considered as an important protection approach by security standards of International Organization for Standardization (ISO) [14], and National Institute of Standards and Technology (NIST) [15].

In [16] for example, A Security Education, Training and Awareness (SETA) was defined as an educational program that aim to reduce security breaches that caused because of the lack of employees' security awareness. SETA was designed to educate employees how to focus on security issues to protect themselves and their organization's data and network. SETA program integrates security in all tasks that employees do; from locking computer screens when they move away from their desks; to report unusual activities regarding to emails, files and staff.

In Anandpara et al's experiment for example did not improve participants' ability to differentiate between phishing and legitimate emails, it however has made them more suspicious (i.e. more aware) [17].

In some cases, education and training are used as synonyms, such in [12] but there is a quite well described difference between the two definition. Education is "the process of teaching or learning the knowledge, especially in a school or college". Training is "the process of learning the skills you need to do a particular job or activity". [1]

Based on this, education on information technology safety may lead a better understanding of SAT, SETA. Building on

the knowledge of the term's vocabulary can lead to better understanding of SAT, SETA projects – which are based on organizations ISA may lead better compliance to it.

Prior to the findings above Nurse et al.'s study formulates "One of the main reasons why users do not behave optimally is that security systems and policies are poorly designed" [18]. At this point we do not agree it with fully. Maybe there are another significant component causes the failure and the low effectiveness of ISP and aligning to it.

III. Technology or Human behaviour

In the study made by Bada et al. finds "Behavior change in a cyber security context could possibly be measured through risk reduction, but not through what people know, what they ignore or what they do not know. Answering questions correctly does not mean that the individual is motivated to behave according to the knowledge gained during an awareness program." [19] which can be an indicator on not only poorly designed and implemented ISP is the matter.

There are two different point of view established in past years in connection with information security awareness and its necessity. First is focusing on technology and driving there is no need on education and training of awareness in higher level. We do not agree with it at this point, because some kind of awareness, specially information technology safety is highly recommended. With this as a baseline common understanding of users or employees, based on risk appetite, it can be completed with technical controls, focusing on the security of the employer's property. But most of these controls are not effective in the employee's personal life and time. "It is recommended that when possible to use hardware or software to implement and enforce policy. The money that is saved by not repeating ineffective awareness messages can be redirected to those awareness areas that are not enforceable by hardware or software. It is also recommended that behavioral-based measurements used to determine compliance." [4]

The second point of view enhances the security awareness and pointing out that awareness is not only matter of knowledge, but behavior, motivation, emotion, interest and culture impacted too. In Al-Omari, et al.'s study the first to address the role of users' general knowledge of information security issues on their attitude to comply with ISPs. The result suggests that an employee's attitude toward compliance with ISP can be enhanced by his/her general security awareness [10] Also they found "that creating security-aware culture within the organization will shape users' attitude and behavior to be more security-conscious".

The real problem with awareness knowledge, education and training is defined in an ISF article: "People know the answer to awareness questions, but they do not act accordingly to their real life" and "Simple transfer of knowledge about good practices in security is far from enough." [11]. Based on these quotes we assume the root of the problem can be highlighted. These problems can be:

- Not properly defined goals of the trainings, materials,
- No base ground defined for the awareness,
- Too narrow or too wide curriculum,
- Not a uniform set of basic knowledge from the audience and
- Not well-defined common understanding on the topic.

Without these prerequisites there is a small chance for the effective training. Findings in support of these can be found in recent studies, like Bada et al.'s article about cybersecurity awareness: "The fact today is that security awareness as conceived is not working. Naturally, an individual that is faced with so many ambiguous warnings and complicated advice, may be tempted to abandon all efforts for protection, and not worry about any danger. Threatening or intimidating security messages are not particularly effective, especially because they increase stress to such an extent that the individual may even be repulsed or deny the existence of the need for any security decision." [19]

A. Information security vocabulary

A new Pew Research Center survey finds that Americans' understanding of technology-related issues varies greatly depending on the topic, term or concept. While a majority of U.S. adults can correctly answer questions about phishing scams or website cookies, other items are more challenging. For example, just 28% of adults can identify an example of two-factor authentication – one of the most important ways experts say people can protect their personal information on sensitive accounts. Additionally, about one-quarter of Americans (24%) know that private browsing only hides browser history from other users of that computer, while roughly half (49%) say they are unsure what private browsing does. [20]

According to the finding above the Pew Research Center pointed out in a follower article: "the typical (median) respondent answered only five of these 13 knowledge questions correctly (with a mean of 5.5 correct answers). One-in-five (20%) answered more than eight questions accurately, and just 1% received a "perfect score" by correctly answering all 13 questions." [21] This may refer there is a lack of basic knowledge of technical vocabulary. Based on this Chan et al.'s finding can be seen in a different way: "Employee awareness levels for the organization are surprisingly low, with employees lacking in both knowledge of concepts and awareness of the organization's policies. The lack of information security awareness was reflected in the admission by many employees that they had previously engaged in behaviors (such as password sharing) which were in direct violation of information security. This may be a result of the lack of policy promotion and enforcement." [9] If the vocabulary or the understanding of the topics are not given to the people – not only for employees – we can not expect consciousness on the security.

IV. A reaction based case

"The tendency for technical experts in the field of information security to tell people what they think they ought to know (and may in fact already know) needs to be recognized as a failure. A common theme from the safety approach is that to achieve effective and efficient communications it is critical to understand the relevant beliefs of the audience. It is not enough to know what behaviors exist that are causing information security risk. Communicators must understand why the behavior is occurring which requires an understanding of an audience's constraints and supporting beliefs." [22] In this study the authors highlighting the Extended Parallel Processing Model [23] which introduces reactions based on fear.

Independently from the studies and researches above, during an information security awareness campaign at an organization we sent out e-mail communication to end-users to raise their awareness on cybersecurity and information security policy. We used the SANS monthly newsletters on Awareness called OUCH! [24]. In first time, the communication of the risks, countermeasures are lay on technical facts. There was no feedback from the end-users of the organization or just a few.

In a case when we sent out a newsletter about ransomware and its capabilities of destruction flavored emotionally, we got feedbacks from our end-users, full of understand of the risk and caution – awareness – on the topic. They highlighted they are touched by the message and they are felt the situation. The message sounded like this: "You can see kidnappings in movies, where the detainees demand a ransom. Imagine that this could happen, kidnapping pictures of your loved ones, your family, from your computer."

Making connections with strong emotions – like fear, love – during communication opened a possibility of an efficient way to enhance the overall information security awareness campaign. This underlines the viewpoint: For information security awareness techniques to improve in effectiveness and efficiency it is clear that information security awareness content can't be created from what the technical experts want to tell people, the contents of a technical standard or the prevailing best practice topics but rather the audience themselves that it seeks to influence and protect. [22]

V. Conclusion

There is a need to separate ISP based ISA from the overall basic Information Technology Security Awareness. An independent definition of Information Technology Safety Awareness is knowledge or perception of a situation or a fact in Information Technology field or related area.

There is a need on education and training of information technology safety where education is "the process of teaching or learning the knowledge, especially in a school or college". Training is "the process of learning the skills you need to do a particular job or activity". The education and the training must be shaped to people and must contain emotional charge instead of dry technology facts.

Based on this, education on information technology safety may lead a better understanding of SAT, SETA. Building on the better understanding, the SAT, SETA projects – which are based on organizations ISA may lead better compliance in information security field.

With this definition we are able to separate and liberate a general knowledgebase from a highly shaped Information Security Policy and its expectations. Narrowing the knowledgebase, we can implement an education model, qualitative and quantitative measurement model and we are able to specify trainings to enhance the education.

Additionally, the awareness message can be delivered to the end-users, the individuals flavored with emotions can help to get their attention and enables them to enhance consciousness.

VI. Future work

We assume there is a need to develop a baseline for information technology safety awareness and create a reference questionnaire to measure the knowledge and emotional base. To complete this, we are going to create a vocabulary baseline and a thematic education material to raise the knowledge base. With this as an education reference there is a good chance to create or maintain ISP based SAT to enhance employee's engagement to comply the recent security awareness requirements.

VII. Acknowledgement

Authors gratefully acknowledges the support of the Applied Mathematics and Applied Informatics Doctoral School on this research.

References

[1] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance. Paper presented at the AMCIS 2009 Proceedings. Paper 419.

[2] Hussain Aldawood, Geoff Skinner: Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE) p62-68 978-1-5386-6522-0/18 ©2018 IEEE

[3] L. Decker, "Factors affecting the security awareness of end-users: A survey analysis within institutions of higher learning," PhD dissertation, School of Bus. & Technol., Cappella Univ., Minneapolis, MN, 2008.Cambirdge Dictionary Online: Awareness, Education and Training, https://dictionary.cambridge.org/dictionary/english/ Accessed: 2020. 08. 21.

[4] Wolf, M., D. Haworth, and L. Pietron, Measuring an information security awareness program. Review of Business Information Systems (RBIS), 2011. 15(3): p. 9-22.

[5] National Institute of Standards and Technology - NIST: Building an Information Technology Security Awareness and Training Program. Wilson, M. and Hash, J. Computer Security Division Information Technology Laboratory. October 2003. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

[6] Siponen, M. 2000. 'A Conceptual Foundation for Organizational Information Security Awareness'. Information Management and Computer Security, 8(1): 31-41.

[7] Information Security Forum (ISF).: The Standard of Good Practice for Information Security, Security Standard. 2007.

[8] Cavusoglu H., Cavusoglu H., Son J.-Y. and Benbasat I. 2008. 'Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers'. UBC Working Paper.

[9] Hong Chan, Sameera Mubarak Significance of Information Security Awareness in the Higher Education Sector International Journal of Computer Applications (0975 – 8887) Volume 60– No.10, December 2012 [6] Al-Omari, Ahmad; El-Gayar, Omar; and Deokar, Amit, "Information Security Policy Compliance: The Role of Information Security Awareness" (2012). AMCIS 2012 Proceedings. 16. http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/16

[10] Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 23.

[11] Information Security Forum (ISF): From Promoting Awareness to Embedding Behaviours, Secure by choice not by chance, February 2014. https://www.securityforum.org/shop/p-71-170

[12] Melad Mohamed Al-Daeef, Nurlida Basir, Madihah Mohd Saudi Security Awareness Training: A Review Proceedings of the World Congress on Engineering 2017 Vol I ISBN: 978-988-14047-4-9 pp446-451

[13] Daintith, John, ed. (2009), "IT", A Dictionary of Physics, Oxford University Press, ISBN 9780199233991, retrieved 1 August 2012

[14] ISO/IEC . ISO/IEC 27001:2005 - . Tech. rep., International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). 2005.

[15] NIST, Nist special publication 800-12, An introduction to computer security: the NIST handbook. 1995: DIANE Publishing.

[16] Hight, S.D., The importance of a security, education, training and awareness program, November 2005.

[17] Anandpara, V., et al., Phishing IQ tests measure fear, not ability, in Financial Cryptography and Data Security. 2007, Springer. p. 362-366.

[18] Nurse, J.R.C., Creese, S., Goldsmith, M., Lamberts, K.: Guidelines for usable cybersecurity: Past and present, in The 3rd International Workshop on Cyberspace Safety and Security (CSS 2011) at The 5th International Conference on Network and System Security (NSS 2011), Milan, Italy, 6-8 September.

[19] Maria Bada, Angela M.Sasse and Jason R. C. Nurse: Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

[20] M. Anderson and E. Vogels, ''Americans and digital knowledge,'' Pew Res. Center, Washington, DC, USA, Tech. Rep., 2019. [Online]. https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/

[21] K. Olmstead and A. Smith, ''Americans and cybersecurity,'' Pew Res. Center, Washington, DC, USA, Tech. Rep., 2017. [Online]. https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/

[22] Stewart, Geordie; Lacey, David: Death by a thousand facts: Criticising the technocratic approach to information security awareness, Information Management & Computer Security, Volume 20, Number 1, 2012, pp. 29-38(10) ISSN: 0968-5227

[23] Delaney, A, Lough, B, Whelan, M and Cameron, M: A Review of Mass Media Campaigns in Road Safety Monash University Accident Research Centre 2004

[24] https://www.sans.org/security-awareness-training/ouch-newsletter