Methodological approach to security awareness

Predrag Tasevski

Security in Computer Systems and Communications
Eurecom, France
e-mail: tasevski@eurecom.fr

Abstract

Currently, humans coupled with the socio-technical aspect can be either the strongest or the weakest link in any information security, and the key in security lies in delivering awareness training through short and effective online videos, whereby the participator can gain knowledge on security. Our aim, therefore, is to develop innovative solutions to deliver an interactive cybersecurity awareness program, where the main goal is to enhance information on security awareness and knowledge in organizations, schools, nations, homes etc. The syllabus that we present consists of a unique systematic approach divided into three target groups: basic, advance and management. Also we present a different method in measuring the knowledge of each participant, and compare it to the base-line survey carried out during the registration. Our results show the participant's awareness level of knowledge. By implementing this program in private and public organizations, governments, schools and universities will lead to the improvement of IT security awareness levels in the everyday use of computers, mobile phones, online banking, and social networking - both at home and in the workplace.

Keywords

cybersecurity, awareness, socio-technical, human factor, syllabus, security

1. Introduction

Nowadays, businesses, organizations and citizens find ICT invaluable for carrying out daily tasks both at home and in the workplace. Analogous to the greater population, organizations and businesses are likely to suffer from security breaches. This is due to vulnerabilities in the new and existing technologies together with device convergence. Such security breaches maybe IT related or may be as a result of incidents caused by human factors. Recent stories have highlighted that a considerable number of end-users are unaware of their exposure to security risk. Through breaches seen recently, it is more critical than ever that organizations raise security awareness by turning users into a first line of defence (ENISA, 2010).

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 to respond accordingly (Wilson and Hash, 2003).

IT security awareness programs are common approaches or models necessary to centralize policy, strategy, implementation and also to distribute the implementation and strategy for a certain, specific organization by improving the information systems in security through implementation of new assets. Moreover, the weakest links can also lie in technologies, implementation of technology and software. Cybersecurity awareness programs are composed of IT security, the flow of information in a crisis, plus the social sphere, for instance social engineering, the human element and social networking. The priorities in cybersecurity awareness programs are to improve the knowledge, and to develop a strategy at the nation level.

While the role of previous studies overlooked the approach and methodologies of delivering effective awareness programs coupled with targeting of different groups (System Security, 2013)(Sémafor Conseil SA, 2013)(SANS, 2013)(IASE, 2013) (eLearnSecurity, 2013), however, there is a lack of specific programs particularly for managers which answer the three important and valuable questions during the creation of security environment awareness program (Spitzner, 2010).

Therefore, in this paper the following study presents the results published in a book (Tasevski, 2013) and the main goal is to embrace awareness at a national level of the weakest element in security by providing a syllabus. The program concerns different target groups and defines the communication concept. Additionally, it defines the goals and objectives of the program. Consequently, it defines the indicator to measure the success of the program and focuses on delivering "*best practices*". Evaluation and feedback mechanisms are critical components of any security awareness program. Thus baseline surveys of the current status are taken beforehand and aim to track the benefits brought about by the awareness program. Evaluation questionnaires were used to solicit feedback from the respondents.

Along these goals, we summarize our main approach and methodology through present findings in order to solve and elevate the level of awareness and knowledge, by positive results as a consequence of the implemented syllabus in schools, universities, private and public organizations.

The rest of the paper is organized as follows: we present the problem and current level of awareness in Section 1.1; Section 2 continues on the curriculum of the syllabus, separated into three parts: basic, advance and management; In Section 3 we note the prototype web solution for a course content management system; finally we then present in Section 4 our results of the syllabus carried out with differences and similarities made by baseline results from the survey and feedback; subsequently we discuss related work in Section 5; we conclude in Section 6.

1.1. Current level of awareness

The focus of the study is to examine primarily the response to the prior concern about the safety and knowledge level for protection of information assets, as well as proposition of already implemented approaches to increase the level of awareness. The survey was conducted among 1000 participants from everywhere, from the age of 11 to 63, within diversity of careers, such as schools, universities, private and pub-

lic organizations.

We can note from the outcome that many of the participants nowadays consider that the safety of their computer is essential. Instead, only 33% of the participants slightly consider protection of peripherals and electronic data as necessary. It is also interesting to note that a greater number of the participants are least concerned about protecting their mobile devices. The participants considered safety as protection from adverse effects, on a scale of one to five; with one being very concerned, and five being the least concerned. Thereby the support for this interpretation comes from Figure 1, where a large percentage of the participants consider themselves somewhat knowledgeable in protecting their information technology assets. There is a marked similarity between the very knowledgeable and least knowledgeable.

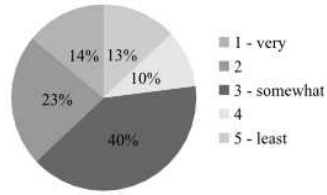

Figure 1: Knowledgeable protection of IT assets - awareness level

Also many organizations, schools and nations are implementing different approaches to increase the level of awareness regarding security. For instance providing a guide (ENISA, 2010) or (Wilson and Hash, 2003). In addition, (SANS InfoSec, 2013) has provided security awareness materials and (University of Arizona, 2013) developed a security awareness site that contains awareness presentations, videos and posters. Further examples are highlighted in the Discussion section.

However, there are enormous differences between each awareness program. Up to now almost all the academic effort in information security training has concentrated on solving the technical and policy aspects of the problem rather than designing security systems and mechanisms to take into account the human factor. Thus resulting in the human factor being the most vulnerable threat in the system. Where in the end this jeopardizes the overall efficiency of the organization and nation.

Nevertheless, new proposals may surpass the actual style of delivering security awareness programs, and (Spitzner, 2010) shares his ideas that the goal is to change people's understanding of risks, and ultimately change their behaviour. The key to having an awareness program that creates a secure environment is answering these three questions: Who? - determines the target of your awareness program; What? - determines the content of what to deliver and teach people; How? - is the means by which you communicate content. Also, many of the existing awareness programs are outdated and use traditional learning methods, such as: presentation, training, etc.

For that reason, we have created a new approach and methodology that determine the answers to the above three questions. The target groups for awareness programs are:

basic, advance and management. We determine the content of what to deliver and teach. Additionally communication is done through short online videos - no more than 10 minutes. And finally, a baseline survey is distributed to measure the beforehand level of awareness to each participant.

2. Syllabus

The program supplies a new systematic approach for different groups: basic, advance and management. Each part contains a certain a number of modules, divided into units, which are pursued into separate chapter/curriculum. The syllabus is built on what we should do and what needs to be done for information security to be safe, either by avoiding or mitigating the security incident. Overall, the idea of the syllabus is to help, improve and elevate the awareness level of three different types of groups of information security. We emphasize that the weakest element is human behaviour, followed by the socio-technical aspect. However, this syllabus does not cover the legal aspects associated with information security matters.

In order for the program to be intriguing, after each unit we supplied questionnaire quizzes, where the participants had to provide an answer. After submitting the answer it is impossible to change the record. Therefore, the participant can only answer the questions once. However, in order to be able to give the correct answer at the bottom of each unit we have a presented a novel approach with additional reading material and hints which will help and guide the participant to procure beforehand the most reasonable answer to the questions. Also after the registration process is completed, the participants are redirected to the baseline survey where the main idea is to measure the knowledge in advance, consequently to examine and note the similarities or difference of gained knowledge, presented in the Section 4.

2.1. Basic

The objectives of the curriculum are to successfully deliver solutions for best practice of using technology. Followed by how to protect personal as well as an organizations information. Moreover to be aware and knowledgeable of how to configure wireless networks for personal benefits and eventually how to understand that you are the victim of an online scam and finally interpret spam filtering. The curriculum is divided into three types of security approaches, such as: physical security, computer and mobile security; and network and Internet security. Firstly, the physical security approach shows very effective methods of protecting your personal and workstation computer, mobile and portable device protection, followed by extremely valuable secure printing issues. In addition, the computer and mobile device security approach deals with the malicious software, operating system security and how to create strong and safe passwords. Lastly, networking and Internet security module is carrying out the effective manipulation and deceiving people issue, such as social engineering and social networking which is important to everyday secure browsing. Solutions on how to identify phishing and perform successful online banking is provided and also identifying annoying spam e-mail and instant messaging messages, followed by firewall and wireless network security, on regular performance.

2.2. Advance

The end users of computers are growing in leaps and bounds. Their control of computers is increasing too. Tutorials, studying, experimenting and learning environments are available for free and they lead to the end users of technology to figure out comprehensive software, and to take full control or functionality of software, network, testing, analysing, developing and so forth. Although the enhancement of technology and Internet suits the daily demands, commitment and performance of advance users, there are many ways to circumvent the defence. In this matter, if the users are advanced or professional in computers, they are aware that they can be targeted as victims or exposed to risks. It is therefore extremely important and favourable that an awareness activity is taken into account by determining that advance users or in other words experts of computers are in fact the ones that can perform and carry out activities such as, configuring networking, programming, troubleshooting issues, installing, etc.

However, this curriculum presents an overall anatomy of an attack and a taxonomy of the tools appropriated in this process; it provides literal scenarios of hacking activities and the solutions of defence against the attacks. Taken as a whole, it provides a reasonable tactical model for the process of sketching and constructing an attack, complemented by a technical overview of the tools, exploiting the steps employed in this process and finally a resolution. The general framework of attacks against computer systems standards are usually described, in approaches such as (Young and Aitel, 2003) and (Skoudis and Liston, 2006) where they aid in delivering the framework, where on the other hand we prefer the curriculum to divide the targeted phase attacks into the following components: reconnaissance, scanning, gaining access, maintaining and expanding access and covering tracks and hiding.

In addition, we supply the participants with additional very attractive and valuable types of attacks, where each type of attack is followed by countermeasures: network scanning attacks, password attacks, exploitation and web application attacks. Alternatively, for the attacking phases and attacking methods, we supply the participants with Advanced Persistent Threat, like anatomy and how to improve resilience to APTs in organizations.

2.3. Management

Information security management is a structured process for the implementation and ongoing management of information security in an organization (Vermeulen and Solms, 2002). It includes activities that aim protecting information and information facilities so as to secure business continuity. It is therefore important that information security management is treated like any vital business function, with all its activities based upon business needs (Kokolakis et al. 2010).

Nevertheless, all managers are users, but on the other hand all users are not managers. In the third and final course of this awareness program we focus and disclose the issues that could arise in the organization intended for the management staff. In fact, we stress the importance of understanding the decision making process espe-

cially nowadays that the management staff in any organization deals with and has to find answers to everyday incidents that arise because of information security.

However, in this Management course we note the phases of the decision making process, in detail by PDCA (ISO, 2009) and OODA (Kapadi et al. 2010) cycle where we included the cost optimization and cybersecurity awareness, as well.

3. Course Management System

For the purpose of this research we have developed a prototype web based application of the syllabus to be available to a worldwide audience.

4. Results

Presently this study provides entrance for participants only with the Basic curriculum and the relevant questionnaire quiz as well as the baseline survey. Overall, the focus of the study is to examine primarily the response to the prior concern about the safety and knowledge of the protection of information assets compared to the scores earned or gained in the curriculum.

In general a large percentage of participants access the internet through different types of broadband communication technology where the usage of the computer is typified. Moreover, the concern about the safety of their information technology assets, such as, the computer and laptop, peripherals, electronic data and mobile devices are aligned and it ranges from extremely concerned to least concerned. Likewise, the range in a scale of extremely knowledgeable to least knowledgeable about protecting their information technology assets is very diverse. Furthermore, the greatest threats to their information technology are by a systematic approach to the most commonly known threats. Thus, the in place protection used for their computer and electronic data is coherent. Additionally, the participants consider viruses, worms, hackers and intruders as the highest threats, instead by malicious software, spam and other unsolicited emails are considered much less significant. Moreover, the participants protect their personal computer or electronic data by anti-virus software that is updated regularly, followed by the firewall. Where on the other hand, the lowest ranking are locked screen saver on their device, anti-spam filter and process of regular backup of data. Last but not least, the participants clearly indicate that online training is the most effective education method of how to protect themselves, followed by the online adverts.

Nevertheless, the basic curriculum consists of three modules, where each module is divided into units. There are a totals of 54 questions in the basic curriculum and the age difference between participants ranges from 11 to 63, where 69% are males and the remaining 31% are females. However, Table 1 of this empirical study is interesting in several ways. First it demonstrates the average percentage score gained from answering the test in each unit from the participants. Secondly it allows us to pinpoint units in which participants are more knowledgeable and in which units they are less knowledgeable so as to take tailored measurements for future actions. Table 1 also presents the average percentage score achieved by users in modules. Such as,

physical security, which indicates 60%, then for computer and mobile security the average score gained by the users in the inside units is 64%, and finally, for the network and Internet security module average score gained by the users is 70%, which is also the highest score.

Table 1 shows that in the physical security module, mobile and portable security unit has the highest score, notably the secure printing unit has the lowest score. Where, in the computer and mobile security module, malicious software and strong and safe password units are practically at the same level with an average percentage score, which is different from the operating system security unit. And in the last module, network and Internet security, the highest average percentage score was obtained in the secure browsing unit.

	Avg. %
Physical Security	59.71%
Protect Your Computer	52.86%
Data Protection	65.09%
Mobile & Portable Security	67.24%
Secure Printing	48.67%
Computer & Mobile Security	63.96%
Malicious Software	67.50%
OS Security	61.96%
Strong & Safe Password	66.05%
Network & Internet Security	70.30%
Social Engineering & Networking	65.38%
Secure Browsing	85.71%
E-Mail and IM Security	57.14%
Firewall	67.14%
Wireless Networking Security	68.57%

Table 1: Basic course, modules and inside units, earned average percent score

The present findings suggest several courses of action in order to solve and elevate awareness level of knowledge, by positive results. Results so far have been very encouraging and they have confirmed that the method and approach of our interactive cybersecurity awareness program are decisive and invincible. The implementation of the syllabus will improve everyday work and usage of computers, mobile phones, online banking and social networking and will also aid in identifying needed future action.

In general, the feedback from participants is that they have found the topics and units interesting. Although many learners had quite a good theoretical background about

the threats of IT assets, they thought it was useful to practice the theory and best known practice. Even a person more competent in computer and mobile security than us, said he was able to learn some new tricks and that the quizzes were exciting. Another detail pointed out was that whilst you may often read about new vulnerabilities or security problems, you usually just don't have enough motivation or time to delve into practical security. In conclusion, we find that the selection of topics is quite effective, although future improvement can be considered. Naturally, we need to keep the list of the themes up to date and seek new and interesting ideas.

5. Discussion and Related Work

Although numerous amounts of awareness programs exist, their approaches and methods are different. The ideas for the awareness program we have implemented are usually not new, but the uniqueness of our awareness program lies in the style of communication, the systematic approach of the targeted groups and the content delivered. Consequently, the uniqueness of our program is coupled with the development of a course content management system and a systematic approach of the scoreboard, the discussion board and tests. The different levels to which this course is applicable, for example, the targeted groups: basic, advance and management adds to its uniqueness. Other unique factors of the program are the baseline survey, because it is applied afterwards and compared to the questionnaire quiz, and lastly the topic advisor which helps the participants and users and gives advice related to their knowledge.

Furthermore, many universities nowadays are carrying out cybersecurity master or bachelor programs. Additionally, different approaches have also been conducted to deliver awareness programs and to boost the level of awareness among the users, employees, even on a national scale. Anyhow, such approaches, that use posters and videos, are (System Security, 2013)(Sémafor Conseil SA, 2013)(SANS, 2013)(IASE, 2013)(eLearnSecurity, 2013) and many others. There are different approaches of measuring information security awareness; however these tend to focus only on the needs of businesses. Such studies are (Kruger and Kearney, 2006) and (Siponen, 2001) where they emphasis the dimensions and the measuring techniques of information security awareness in different target groups particularly to individual and business awareness needs. This differs from our focus on the empirical socio-technical aspects.

All of those listed above and many others have different views and approaches to delivering awareness programs. Few of them, have been developed with the demonstration of awareness through the use of short videos, furthermore, none of them have utilised the questionnaire quiz techniques or measured the prior baseline knowledge before the participants enrolled in the program. Additionally, none of them have developed a topic advisor / mentor for a follow-up action. All of which are essential to determining a target group and audience. On the contrary, this study addresses all of these issues and also brings a broader spectrum of main threats: physical security; computer and mobile security issues; followed by the network and Internet problems. Lastly for managers we have noted and illustrated the necessary decision making process. Indeed every manager is a user, but every user can not be a manager.

We believe that no other previously related work as mentioned above has used such a systematic approach, methods and targeted specific groups of distributing the awareness program as we have done.

6. Conclusion

The threats to cybersecurity are constantly evolving. Thus we need to ensure that not only the specialists who are protecting IT systems get a proper awareness education, but also the basic, everyday users and managers should too. Thereby, only significant changes in user perception, culture and education can effectively reduce the number of information and cybersecurity breaches. Consequently this will raise the awareness level of the human factor in using technologies in everyday life, as well.

Therefore, in this paper we present a set of educational tools and a practical syllabus to support information security awareness using the obedient approach and to help in the development of information that can raise the awareness of the importance of cybersecurity.

The strength of our work lies in the results and the evidence from this study points towards the necessity of implementing the syllabus which will improve everyday work and usage of computers, mobiles, online banking, social networking, and so forth.

We believe that our approach could be implemented effectively in private, public organizations, military, nations, schools and campuses, without a significant degradation in performance. Future studies should examine broader views on policy and legal aspects.

7. References

Apu Kapadia, Joshua Haines, Michael N. Gagnon, John Truelove and OrtonHuang. Isarcs (2010), *Towards Net-Centric Cyber Survivability for Ballistic Missile Defense*, June 23-25.

Clive Vermeulen and Rossouw Von Solms (2002), *The information security management toolbox – taking the pain out of security management*, Information Management & Computer Security, Vol. 10 Iss: 3, pp.119 - 125.

Ed Skoudis and Tom Liston (2006), *Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, Prentice Hall, Jan 2.

eLearnSecurity (2013), Training Provider, http://www.elearnsecurity.com/, (Accessed 16.10.2013).

European Network and Information Security Agency - ENISA (2010), *A users guide: How to raise information security awareness*, Nov 29.

H.A. Kruger, W.D. Kearney (2006), *A prototype for assessing information securityawareness*, Feb.

IASE (2013), IA Education, Training and Awareness, http://iase.disa.mil/eta/, (Accessed 16.10.2013).

ISO copyright office (2009), *Information technology, Security techniques, Information security management systems*, Overview and vocabulary, INTERNATIONALSTANDARD ISO/IEC 27000, .

Lance Spitzner (2010), *How to build an effective information security awareness program*, October.

Mark Wilson and Joan Hash (2003), *Building an Information Technology Security Awareness and Training Program, Computer Security*, NIST Special Publication 800-50, October.

Mikko T. Siponen (2001), *Five Dimensions of Information Security Awareness*, June.

Predrag Tasevski (2013), *Interactive Cyber Security Awareness Program*, LAP LAMBERT Academic Publishing, Aug 10.

SANS InfoSec (2013), Reading Room, http://www.sans.org/reading-room/whitepapers/awareness/, (Accessed 18.10.2013).

SANS Securing the Human (2013), Security Awareness for the 21st Century, http://www.securingthehuman.org/, (Accessed 16.10.2013).

Sémafor Conseil SA (2013), Cyber security awareness campaign, http://goo.gl/FLoiUO, (Accessed 16.10.2013).

Spyros Kokolakis Aggeliki Tsohou, Maria Karyda and Evangelos Kiountouzis (2010), *Analyzing information security awareness through networks of association*, Springer Berlin Heidelberg, August 30-31.

Susan Young and Dave Aitel (2003), *The Hackers Handbook: The Strategy behind Breaking into and Defending Networks*, Auerbach Publications, Nov 24.

System Security (2013), Software and Systems Security, http://www.cs.ox.ac.uk/softeng/security/, (Accessed 18.10.2013).

University of Arizona (2013), Security Basics for Computer Users, http://security.arizona.edu/basics, (Accessed 19.10.2013).