Thriving on Future Education, Industry, Business and Society
15–17 May 2019
Piran • Slovenia
make learn
TIIM
Management, Knowledge and Learning
International Conference 2019
Technology, Innovation and Industrial Management

HOW TO DEAL WITH THE AWARENESS OF CYBER HAZARDS AND SECURITY IN (HIGHER) EDUCATION?

Moti Zwilling
Ariel University Israel
motiz@ariel.ac.il

Dušan Lesjak
International School for Social and Business Studies, Slovenia
dusan.lesjak@guest.arnes.si

Srečko Natek
International School for Social and Business Studies, Slovenia
srecko.natek@vizija.si

Kongkiti Phusavat
Kasetsart University, Thailand
fengkkp@ku.ac.th

Pornthep Anussornnitisarn
Kasetsart University, Thailand
fengpta@ku.ac.th

Abstract:
Cyber Security of information systems and infrastructure has turned out to be one of the most important issues in recent years. Many people, both children and adults, use portable devices such as mobile phones and tablets in their day to day life, to access computer networks that are connected through the Internet. However, as internet use includes the use of many tools that use shared applications, such as navigation, access to information, trends in social networks, news content, entertainment and office applications (e-mail, calendar, etc.), it has also become an arena for hazards such as user identity theft, privacy sabotage, malicious code, cyber bullying and others. Whilst cyber security has been researched in the literature, few studies addressed cyber security awareness and users' indifference in cyber security behavior. Moreover, the awareness of cyber security threats among various clusters of users (such as IT experts vs. non-experts, older vs. younger users) has not been fully evaluated.
The aim of this paper is to enhance cyber awareness of individuals and thereby equip and prepare them for safer and better work and life, by providing theoretical and practical solutions related to cyber security awareness of various clusters of users, such as elementary and secondary school children, students, employees and retired people.
Therefore, the objectives of this paper are as follows:

1. Develop recommendations for curricula changes at each level of the evaluated education systems and practice.
2. Develop a cyber awareness education framework (CAEF) using suggested recommendations for curricula changes at all levels of education.

We expect to understand which factors are involved in the cyber awareness gap and how to narrow or even eliminate the gap through specific recommendations, i.e. how to improve the cyber awareness of individuals in the curricula at various levels of the education system.

Keywords: cyber crime, cyber security, cyber awareness, education, higher education

1. INTRODUCTION

As cyber use becomes increasingly popular amongst individuals with different levels of knowledge of information technology, the gap between older and younger users related to cyber hazards is growing significantly. For example, the rate of cyber bullying victimization jumped from 18.8% in 2007 to 27.32% in 2010 (Hinduja and Patchin, 2014). Following this gap, Bong-Hyun et al. (2016) demonstrated the importance of developing an Internet-based cyber education/training system. The need to develop a system based on the level of user awareness was also asserted by Dodel and Mesch (2017). Their study used a health belief model (HBM) approach as a predictive model for cyber-victimization preventive behaviour. In this study the authors claimed: "We believe that the findings also signal the need for further research using the HBM as the basis for understanding cyber-safety. The role of previous victimization incidents is not clear, perhaps its impact is mediated through awareness…or it may be that future studies should focus only on past actual damage, not just victimization episodes."
A recent study by Lukanović (2017) on a sample of more than 200 Slovenian Internet users found that 83% of respondents had experienced a computer virus infection. The author of this study also reported that just under one third of respondents' friends experienced computer hacking and online identity theft and that they know at least one person who was harmed by cybercrime. On the other hand, the author reported that approximately one half of respondents have sufficient information to protect themselves against the misuse of their personal data; however, 40% of them did not know or did not install any software protection on their Internet-connected devices (computer, phone, etc.). Another study, conducted by Rek and Milanovski (2017) on a sample of more than 800 Slovenian secondary school students aged 15 to 18 emphasized the need for cyber educational programmes in a time of increasing cyber hazards. It was found that only a few of the participants check URL address of the web pages they tend to visit or check its credibility. In addition, many of them are open to publicly sharing details of their personal life and are not aware of the potential exploitation of such data.
Security threats have been shown to have a negative impact not only on the assets associated with an organization but also on its reputation. Dahbur et al. (2017) examined private and public organizations in Amman and showed that security awareness levels are similar for all positions and for all levels of employment. The authors stated that it is necessary to raise cyber security awareness already as part of secondary education in order to provide the market with well-trained employees with a high awareness of IT security issues. The authors recommended a development of a programme "tailored" to industrial organizations. From all of the above, we observe that cyber hazards have become a real threat to a variety of users who hold, use and expose themselves to a device whilst using the Internet to run applications and participate in social network discussions. Cyber bullying is just one of the main hazards among many others that emerged with the increased trend of technology use for various purposes. This trend demands enhancement of cyber awareness among users, incorporating face-to-face and computerized training.
Awareness and training have a significant combined impact on cyber security level. McCrohan et al. (2010) examined users' passwords and ways of securing computers pre and post cyber security training. The authors stated the importance of cyber education/training on cyber threats and emphasized the need for appropriate security practices that will change the behaviour of online users in their day-to-day practice. Following McCrohan (2010), Abawajy (2014) explored user preferences regarding cyber security awareness delivery methods. The author showed that cyber education/training is divided into several categories depending on delivery method: online training, contextual training and embedded training. The author concluded that the combination of delivery methods (such as text-based, game-based and video-based) determines the training type. Later on, Pawlowski et al. (2015) examined students' concerns about cyber security threats and identified 23 concepts forming the understanding of cyber security. The authors advised that cyber security courses should be treated as problem-centred, utilizing case studies that are tailored to students' level of awareness. In order to develop a practice plan for cyber security education, Harris and Patten (2015) developed a cyber security taxonomy that allows moving security issues form higher-level courses to lower and intermediate ones. Their IT security taxonomy was based on Bloom and Webb's taxonomy, which is used in this study.
Cyber security awareness in Europe became in general more transparent with GDPR - General Data Protection Regulation (European Parliament and Council, 2016) when European citizens recognized the deep meaning and commercial value resulted from their personal and transactional data for IT services provided to firms e.g. browsers, social media, data providers, sales profilers, etc.
In the recent years, artificial intelligence and particularly data mining algorithms for business analytics (Shumeli et al., 2018) have turned to be an integral part of contemporary transactional applications e.g. global product selling which uses linear regression models for sales prediction to manage the sales promotion or a focused advertising, based on preference and personal data, spam filtering that uses a

Naïve Bayesian classifier to analyze the content of the spam mail using in addition text mining analysis, Classification and Regression tree for consumer's behavior classification and many more. The processed data is usually sold out to trading companies or transferred directly to big firms. Since data is produced from many computerized devices – from mobile phones applications through the massive usage of internet web services the behavior of many users in the daily process of applications usage is considered as very common and their awareness to the resulted risk is still under question and should be deeply evaluated.

2. THE RELEVANCE OF THE TOPIC

This paper is the first attempt to shed light on the level of awareness of cyber hazards amongst a variety of users (young and old; studying, working and retired) who use their computer devices (either desktop or mobile) in their everyday activities. The authors advance calls for further research, identified in the latest publications in this field.

The importance of this paper arises from the rapid development and the variety of applications that utilize the Internet when activated, such as applications for storing data in the Cloud, storing and retrieving user profiles, etc. These applications are used extensively by a variety of users, who, as a by-product, are exposed to cyber hazards, since many of these applications have vulnerabilities and are exploited by hackers to hack user computers, steal their identity, their personal data for the purpose of cyber bullying, etc. In most cases, users are not aware of these hazards at all as part of their day-to-day use. Nevertheless, such hazards can be monitored automatically by cyber defence technologies that users should install on their devices; however, since most users are not IT experts, or do not have the ability to inform themselves about becoming a victim of a cyber-attack, they need to be exposed to an appropriate education programme, in order to acquire the "tools" and knowledge to understand which technology to install on their devices and which cyber hazards they need to be aware of. In other words, most users need to acquire sufficient cyber-related knowledge through courses, workshops and computer-based training tools, such as game-based learning, videos and written information. We believe that the suggested approach is relevant and sustainable to prevent users to urgently disconnect from the internet if there will be no other rescue option. Especially since artificial intelligence (AI) is important and embedded part of cyber-attacks and depends deeply on internet connection and many users are not aware to the usage of AI by hackers in order to steal, intrude into the users computers in order to steal data, or install malware that later could be used for ransom demands from the users.

Following from all of the above, we believe that the proposed study, which provides face-to-face, as well as computer-based cyber training, alongside constant monitoring of user behaviour in the cyber arena and real-time alerts, is important as it contributes to netizen social development.

3. THE CYBER AWARENESS AMONG ISSBS STUDENTS

A paper-based survey was distributed in 2017 among bachelor and bologna master students at the International School for Social and Business Studies. The subjects were located through convenience sampling. In the Table 1 you can find their characteristics.

Table 1: Characteristics of the sample

Gender		Study cycle		Type of a study		Field of a study	
Female	25	bachelor	11	Part-time	9	Management	20
Male	10	master	24	Full-time	26	Economics	15

As we can see from the Table 1. Most of the participants were female, at the bologna master level, mainly full-time student, studying social studies, precisely, management and economics, what is quite a good example of the bologna master studies in the field of social sciences, where we in Slovenia are having more than one third of the students at that level. Yet is should be noted that the sample size is quite small (over whole 35 participants) which may require more analysis in future studies to understand its implications on the whole population.

The questionnaire included several questions that aimed to test the global familiarity of the subjects to cyber security in general as well as specifically to test the level of awareness to cyber security risks. The questionnaire also explored which operations for cyber security defense were managed by the subjects, the attitude towards attending cyber security training programs to more cyber focus behaviors, such as installing specific cyber security defense tools on their devices and acquiring new

defense tools and knowledge. Each respondent was also being asked about former knowledge in cyber, internet usage and cyber security experience. Classification was conducted according to the level of their cyber security awareness (*Awareness*), their familiarity with cyber security incidents, their knowledge of cyber security and cyber threats (*Knowledge)* and their attempts to control and prevent cyber-attack (*Behavior)*.

Table 2: Descriptive statistics of the answers

Name of Variables	Description/question	Mean	St. Dev.
Awareness	Are you familiar with the term cyber security? (1-no knowledge to 4-very good)	2.57	0.60
Familiarity	Familiarity of different sources (range from 0 sources through 9 sources)	4.85	2.36
IT security training	Would like to attend in IT security training? (1- definitely not to 5- definitely yes).	3.97	0.85
Threats	The main cyber security threats are: (1-strongly disagrees to 5- strongly disagree)	4.00	0.86
Education awareness	The extend in which the current education influenced their cyber-security awareness (1-definitely not affected to 5- strongly affected)	3.40	0.95
Behavioral	I know how to behave in case of cyber-attack (1- defiantly no to 5-rather yes.)	3.17	1.20
Protection	Sum of the score in the usage that the responders make to protect their instrument (ranged from 0 to 11)	5.60	2.39
Length	The average length of your standard password (minimum 0 to maximum 14)	10.49	3.85
Password	Do you use the same password for different portals, system and application	34.3	
Finish	Sum of the activities that the responders are acting when finish working on the computer (ranged from 0 to 4)	1.48	0.88

The students, who participated in the research evaluate their skills and knowledge in using computer application on the average with the 3.16 (from 1-no skills to 5-very high skills), therefore we would label them as average computer users. Interestingly, being asked whether they use the IT product because of their desire or by coercion, their average is 3.11 (1-definitely by coercion to 5 definitely by choice), meaning that apparently not all of them use IT products that are chosen by desire.

As we can see from the Table 2, most of the respondents are to a certain extend familiar with the term cyber security (Mean 2.57) and among the 9 sources of the cybercrime, they on the average are familiar with almost 5. In addition respondents are quite aware of cyber security threats such as viruses, Trojan horses and many more malwares (Mean = 4.0). Moreover, most of the participants of the research would like to attend IT security training (Mean = 3.97) and they believe to a certain extend the current education influence their cyber-security awareness (Mean = 3.40). Obviously from the analysis of the results it turns out that we have to provide a specific and tailored made education that is focused on more info and skills such as a how to deal with the cyber-crime and security threats in the digital arena.

The participants of the research to a certain extend believe that they know, how to behave in case of a cyber-attack (Mean = 3.17), what should be further investigated to evaluate, whether they have a correct justification, yet we do believe that this is just one aspect which is focused and specialized on training and education which definitely have a positive impact on how to construct the needed framework for the training process among the participants.

Regarding the protection of their “instruments »we need to do more, to help them, i.e. focus on training and delivery of the knowledge exists related to the cyber security hazards. More on that could be done on promoting the awareness of installing protection tools against malware (anti-virus), Firewalls, etc.

Regarding the usage and protection of their passwords, it turns out that they obtain the average of above 10 characters, what is usually a consequence of the needed at least 8 character password, yet what is concerning is the fact that one third of them are still using the same password for different purposes.

An important aspect that strengthen the need for cyber security training can be seen from the item in which we asked the participants what do they do when finishing working with their computers (Mean = 1.48). The question simply wanted to examine whether users which are not qualified with the cyber security and technology shut down their commuter or at least log off from the user account when the work with their computer is ended. Results show that most of them do not perform the requested

activities (Shut down, close the account by logging off), rather they prefer to lock their computer or not to do anything (since Mean = 1.48). This result is a good indication for the need of training and increase the awareness of users to be more cautious when they leave their office at the end of the working day especially with the whole activities related to their computer device.
To conclude, the results of this mini research among the ISSBS master students reveals that there is a need and a space for improvements regarding the cyber awareness, which at least higher education could and should provide.

4. COMPUTER AWARENESS EDUCATION FRAMEWORK (CAEF)

As the need for computer awareness education rises, we recommend on developing the following framework for the knowledge improvement among students and targeted audience:

1. Review the theoretical literature in order to develop a robust framework for so called Cyber Awareness of Individuals (CAI) considering the 8 proficiency levels (Carretero et al., 2017). This framework should be composed of different groups of variables related to several evaluated themes - Technology, Education, Demographics and Awareness. Each theme contains several variables:
   - Technology variables: level of device usage, safety, and content of data.
   - Education variables: willingness to acquire new knowledge about cyber hazards, problem solving, and willingness to implement cyber applications patches.
   - Demographic variables: personality traits and preferences.
   - Awareness variables: level of awareness of cyber hazards. The awareness group will be attributed as dependent variables, whereas others groups will contain the independent ones.
2. Conduct a comprehensive analysis of a country formal education systems (from elementary schools to universities and short-term programmes for companies). In addition, evaluate how cyber awareness is presented and delivered in a particular country.
3. Conduct In-depth interviews with various clusters of respondents (IT and other experts) , about individual devices and services (such as torrent, social media, etc.) with the purpose of demonstrating different types of IT use and applications and the levels of exposure to cyber hazards as a result of this use.
4. Based on the interviews, a validated questionnaire to examine the level of cyber awareness amongst the evaluated respondents should be developed and evaluated. This questionnaire should take into account existing questionnaires that dealt with cyber security awareness; for example, the one by Ling et al. (2016), which validated the relationships among peer behaviour, cue to action and employee behaviour in case of cyber security threats. In addition, the so called Health Believe Model (HBM) approach should be used as a basis for a questionnaire instrument. Using the questionnaire, a survey should be conducted among several clusters based on age and industrial sector. Each cluster should contain additional demographic attributes, including age, gender, education, profession and risk. The sample should contain at least a couple of hundreds respondents in each cluster. A simple random sampling method could be used and a descriptive and non-descriptive comparative analysis should be conducted.
5. Develop and perform a curricula changes at each level of the evaluated education systems and practice, and presentation of these at different seminar for various stakeholders.
6. The CAEF is expected to contain written recommendations for curricula changes at each level of the evaluated education systems. The CAEF should also include "tailored" courses for the business sector, which should be created together with senior management as a response to the level of cyber risk and organizational structure.

This framework would assist in building the tailored syllabus. The next stage would be to perform an execution related to the syllabus content as defined by the framework by theoretical and practical courses provided by higher education institutions.

5. INSTEAD OF CONCLUSION

The expected contributions of CAEF are:

- From a **scientific point of view**, the paper elaborates on the existing knowledge related to cyber hazards, providing a theoretical framework for cyber awareness, a practical example to evaluate the level of cyber awareness in a variety of clusters of users, and a practical cyber awareness educational framework, which could be applied both in academic institutions and schools through face-to-face courses and workshops, as well as through a training software provides "targeted" materials for various levels of users according to their IT knowledge and their calculated risk of being

a victim of cyber hazards.

- From a **social viewpoint**, the paper contributes to the creation of a well-educated society of users with different levels of IT knowledge. The paper might be furtherly developed especially important in relation to :"weak users", hence: users with less awareness and knowledge to cyber hazards, such as children with special needs and older people, as it is assumed that the lack of cyber hazards awareness among these groups increases exponentially each day and it is expected that more funding and effort will be invested in educational programmes and prevention of cyber exploitation in the form social engineering, identity theft, etc. amongst these groups.
- From an **economic point of view**, we believe that cyber awareness education, which would take into account the recommendation of the paper will guide both businesses and organizations on how to enhance the awareness of cyber hazards amongst their employees, and education institutions on how to build cyber awareness education/training programmes more efficiently, reduce costs as well as the level of existing risks and the level of exposure of the organization to cyber-attacks due to a lack of employee knowledge and awareness of cyber threats. In other words, we believe that the investment in cyber security education especially for the industry enhance the cyber awareness among employees and managers could save many firms from the need to spend unnecessary money to recover from a cyber security disaster. A training session that is focused on the knowledge gap related to cyber security among employees and managers could also contribute to the firm by increasing the strength of the firm to handle cyber security incidents.

In this paper we propose a practical education approach aimed at evaluating the impact of cyber education on the level of cyber awareness of individuals, to enhance individual awareness of cyber hazards and to deduce the level of cyber victimization amongst users. The approach is generic and could be used by academic practitioners to design the needed syllabus content to their target audience according to the level of expertise and familiarity with cyber security items.

REFERENCE LIST

1. Abawajy, J., (2014),"User preference of cyber security awareness delivery methods", Behavior& Information Technology, 33(3), 236-247.
2. Bong-Hyun, K., Ki-Chan, K., Sung-Eon, H. and Sang-Young., (2017), "Development of Cyber Information Security Education and Training System", Multimed Tools Appl., No. 76, pp.6051-6064.
3. Dahbur, K., Bashabsheh, Z. and Bashabsheh, D., (2017), Assessment of Security Awareness: A Qualitative and Quantitative Study, International Management Review, 13(1), 37-58.
4. Carretero, S., Vuorikari, R. and Puni, Y., (2017), "The Digital Competence Framework for Citizens with eight proficiency levels and examples of use", Publication office of the European Union, doi:10.2760/38842.
5. Dodel, M. and Mesch, G., (2017)"Cyber-victimization preventive behavior: A health belief model approach", Computers in Human Behavior, 68, 359-367.
6. European Parliament and the European Council. 2016. GDPR. General Data Protection Regulation. Directive 95/46/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679 (21. 3. 2019)
7. Harris, M. and Patten, K., (2015),"Using Bloom's and ouWebb's Taxonomies to Integrate Emerging Cyber Security Topics into a Computing Curriculum", “Journal of Information Systems Education”, 26(3), 219-234.
8. Hinduja, S. and Patchin, J. W., (2014)," Cyber bullying Identification, Prevention, and Response". Cyberbullying Research Center (www.cyberbullying.us). [https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response.pdf]
9. Ling, L., Xu, L., He, W., Chen, Y. and Chen, H., (2016), "Cyber Security Awareness and Its Impact on Employee's Behavior", International Conference on Research and Practical Issues of Enterprise information systems (CONFESIS), 103-111.
10. Lukanović, L., (2017), "Računalniška kriminaliteta in varstvo osebnih podatkov: diplomska naloga". Available at: http://www.ediplome.fm-kp.si/Lukanovic_Lea_20171017.pdf
11. McCrohan, K. F., Engel, K. and Harvey, J. W., (2010),"Influence of Awareness and Training on Cyber Security", Journal of Internet Commerce, 9(1),23-41.
12. Pawlowski, S. and Yoonhyuk, J., (2015), "Social Representations of Cyber security by University Students and Implications for Instructional Design", Journal of Information Systems Education, 26(4), 281-294.
13. Rek, M. and Milanovski, B.K., (2017),"Mediji in srednješolci v Sloveniji 2016 [datoteka podatkov]. Slovenija, Ljubljana: Fakulteta za medije [izdelava], 2016. Slovenija, Ljubljana: Univerza v Ljubljani, Arhiv družboslovnih podatkov [distribucija]", IDNo: MPSS16.
14. Shmueli, G. Bruce, P.C. Yahav, I. Patel, N, R. Lichtendahl, K., C. Jr. (2018), Data Mining for Business Analytics. Concepts, Techniques, and Applications in R. Wiley.