https://doi.org/10.48009/1_iis_2019_80-87

Issues in Information Systems
Volume 20, Issue 1, pp. 80-87, 2019

CYBER CRIME AND CYBER SECURITY AWARENESS AMONG STUDENTS: A COMPARATIVE STUDY IN ISRAEL AND SLOVENIA

Dušan Lesjak, University of Primorska, Faculty of Management Koper and ISSBS Celje
dusan.lesjak@fm-kp.si
Moti Zwilling, Ariel Universit, Department of Economics & Business Administration, Ariel
motiz@ariel.ac.il
Galit Klein, Ariel Universit, Department of Economics & Business Administration, Ariel
galitk@ariel.ac.il

ABSTRACT

In this paper we present the results of a survey that examined the attitude of users to cyber crime as well as their awareness of cyber security threats. The study was conducted among Israeli and Slovenian students. The study results reveal significant differences in the level of cyber awareness between evaluated groups of cyber users in both countries. The results may serve as the initial phase of a practical education approach aimed at evaluating the impact of cyber education on the level of cyber awareness of individuals. The study implication can also be utilized for the process of development courses to enhance individuals' awareness of cyber hazards and to reduce the level of cyber victimization amongst users. Finally, the paper's findings contribute to a better understanding of which factors are involved in the cyber awareness gap.

Keywords: cyber crime, cyber security, cyber awareness, higher education, students, Israel, Slovenia

INTRODUCTION AND BACKGROUND

The usage of technology in general and cyber security technology in particular, over the internet, had turned many users to become more aware of cyber hazards. Nevertheless, since there is still a huge difference in the levels of knowledge related to information technology (IT) and cyber security, such as the gap between elderly and young people, in order to provide more attention and solutions to overcome the existing gap where cyber hazards are apparently growing significantly, a survey should be conducted. Cyber hazards are ranged from cyber bullying victimization, which jumped from 18.8% in 2007 to 27.32% in 2010 (Hinduja and Patchin, 2014, Benshalom et al, 2017), to ransomware and identify theft. In 2016, Bong-Hyun et al. (2016) was one of the first researchers that identified the lack of awareness of many internet users when it comes to different types of hazards. In his study he emphasized the importance of developing an internet-based cyber education/training system in higher education institutions in order to mitigate the gap between the existing knowledge of users to the desired one in comparison to the increase in complexity and mode of action of many cyber risks. The need to develop a system based on the level of user awareness to assist individuals in understanding and changing their behavior related to cyber risks 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 behavior. In this study, the authors among other claimed the following: "We believe that the findings of this study 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 yet well clear, perhaps its impact is mediated through awareness…or it may be that future studies should focus only on past actual damage, not just on victimization episodes". Dodel and Mesch (2017)

During the years, more studies not only focused on the various usage of technology that exposes people to cyber risks but also on different approaches that can be delivered to users by different types of means in order to increase their awareness to cyber hazards. For example: the study of Lukanović (2017), conducted on a sample of more than 200 Slovenian Internet users, revealed 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 reported knowing at least one person who was harmed by cyber crime. On the other hand, the author reported that approximately one half of respondents have sufficient information to protect their devices misuse or personal data theft/. However, it turned out that 40% of them did not know or did not install any software protection on their Internet-connected devices (computer, phone, etc.). In the same year, a following study, conducted by Rek and Milanovski, (2017) on a sample of more than 800 Slovenian secondary school students aged from 15 to 18, emphasized the need for cyber educational programmes,

especially in higher education institutions in a time of increasing cyber hazards incidents. The study had shown that only few participants check URL addresses of the web pages they tend to visit or check their credibility/. In addition, many of them are open to publicly sharing details about their personal life (provocative content) and are not aware of the potential exploitation of such data by hackers, criminal organizations or unknown users.

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 example of the many hazards that had emerged with the increased trend of technology use for various purposes. This trend demands enhancement of cyber awareness among users, incorporating face-to-face discussions and training with cyber security incidents via computerized systems.

Awareness and training have been characterized as having a significant combined impact on the level of cyber security exposure among users. For example: McCrohan et al. (2010) examined users' passwords and different ways of securing computers pre and post cyber security training sessions provided by various academic and industrial programmes. The authors mentioned the importance of cyber security training programmes that can change the attitude and behavior of internet users, by decreasing the number risk affiliated with cyber security incidents. The authors also pointed out the need for appropriate security practices that will change the behavior of online users in their day-to-day practice. Following McCrohan (2010), Abawajy (2014) explored user preferences regarding cyber security awareness delivery method. The author showed that cyber education/training can be divided into several categories depending on the delivery methods: 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. Cyber education was also evaluated by Son et al. (2015); their study confirms that cyber security teaching can be organized in different ways. The authors described the process of integrating security labs into the curriculum in three forms: a pure virtual lab, a traditional physical lab, and as a hybrid approach. They concluded that security labs should be an essential part of the curriculum; however, the deployment model should be based on individual institutional requirements. In order to develop a practice plan for cyber security education, Harris and Patten (2015) developed 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's and Webb's taxonomy, which is utilized by the author of this study as part of the methodology.

In this study we present the results of a survey aimed to the test the awareness among Israeli and Slovenian students and examine how education system may serve as the initial phase of any practical education approach aimed to increase the level of cyber awareness of individuals, through a process of unique courses that focus on cyber security, in order to enhance awareness and mitigate the level of cyber victimization amongst users.

The importance of this survey 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 side-effect, are exposed to cyber hazards. Moreover, many of these applications have vulnerabilities as well, such as being exploited by hackers to hack users' computers, steal their identity, their personal data for the purpose of cyber bullying, etc. In most cases, users are not at all aware of these hazards as being a part of their day-to-day use of the internet technology. Nevertheless, such hazards can be monitored automatically by cyber defence technologies that users should install on their devices. Another important issue derives from the fact that the majority of users are not IT experts, or do not have the ability to be aware to the fact that they had turned to be a victim of a cyber attack. This is one of the reasons that such users should be more exposed to an appropriate education programme, where they could acquire the "tools" and the needed knowledge to understand cyber hazards, for example: 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.

THE RESEARCH

Purpose, objectives and results

As stated before, the aim of this study is to enhance cyber awareness of individuals and thereby prepare and equip them for safer and better work and life, by providing theoretical and practical solutions related to cyber security awareness of various users, firstly by focusing mainly on students in both countries: Israel, which is known as a

"cyber nation", and Slovenia, which, on the one hand, is very similar (size, few ethnic groups, few religions, and particularly a very high Human Development Index) and, on the other hand, very different (population, GDP per capita, etc.) compared to Israel.

The survey is the first attempt to shed light on the level of awareness of cyber hazards amongst students who use their computer devices (either desktop or mobile) in their everyday activities. No comparison has been conducted between the two countries related to cyber threats behavior among internet users. However, as part of the analysis of this study, we described the daily internet usage behavior of respondents from both countries and tried to evaluate whether this behavior is similar or different and in what ways. The daily internet usage of the respondents was among other surveyed by asking about their mobile usage and their static ICT devices.

The motivation for this study derived from the literature survey, where many studies mentioned the need to develop cyber security awareness programmes for internet users due to many hazards evolved from using the internet without sufficient awareness. The study focused on two research questions:
1) What is the level of users' cyber security awareness among internet users in both countries and
2) Which kinds of behavior skills are affiliated with this awareness?

The survey was conducted in two countries: Israel and Slovenia. Its implications could be used to develop cyber security awareness programmes in those countries provided by higher education institutions. The study was conducted on a randomized sample of BA and Master students.

We expected to find significant differences in the level of cyber awareness between the evaluated groups of cyber users in both countries. We also expected to understand which factors are involved in the cyber awareness gap and how to narrow or even eliminate the gap by using specific tools or programs. By considering study programmes, we evaluated the need to improve the computer awareness of individuals in the curricula at various levels of the education system.

Method
For the survey related to cyber awareness of individuals, we developed and used a questionnaire, which included several questions aimed to test the global familiarity of the subjects to cyber security and technology 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, their attitude towards attending cyber security training programs as well as focusing on their behavior with internet based technology in the sense of weather they install specific cyber security defense tools on their devices and whether they acquire new defense tools and knowledge to handle the existing cyber security risks. Each respondent was also being asked about former knowledge in cyber, internet usage and cyber security experience.

Classification of the answers was conducted according to the following:
- The level of their cyber security awareness (*Awareness*),
- User's familiarity with cyber security incidents, their knowledge about security threats (*Behavior)* and
- User's attempts to control and prevent cyber-attack (*Behavior)*.

Characteristics of the Sample
To deliver the questionnaire to different respondents from the tested countries, an internet English version of the questionnaire was uploaded to a web site. The link to the site was distributed by each of this study's authors to the respondents during one of the BA or MBA courses that were taught by the authors during the academic year 2017-2018. The subjects were located through convenience sampling. Overall, the sample included 124 subjects who participated in the survey, among students from the department of Economics and Business Administration at Ariel University in Israel (n= 89), and BA and MBA students at the International School for Social and Business Studies from Celje in Slovenia (n=35). The questionnaire included confirmed questions taken from different studies in the literature, for example: Lukanović (2017), Rek and Milanovski (2017), Pawlowski et al. (2015). The questionnaire questions were adjusted and enhanced for the survey, conducted in our research.

The data was collected automatically to Excel through the electronic internet questionnaire and analyzed by the SPSS™ Software.

We gathered the following data from the respondents in the survey: gender, level of study, type of study as well as study fields.

Table 1. Characteristics of the sample

Characteristics of participants		**Total**		**Israel**		**Slovenia**	
		#	**%**	**#**	**%**	**#**	**%**
Female		69	55.6	44	49.4	25	71.4
Male		55	44.4	45	50.6	10	28.6
Total		124	100.0	89	100.0	35	100.0
Level of study	Bachelor	84	67.7	73	82.0	11	31.4
	Master	36	29.1	12	13.5	24	68.6
	Ph.D.	4	3.2	4	4.5		
Type of study	Part-time	35	28.2	26	29.2	9	25.7
	Full-time	89	71.8	63	70.8	26	74.3
Study field	Economics	51	41.1	36	40.4	15	42.9
	Business & Management	41	33.1	21	23.6	20	57.1
	ICT& Logistics & Other	32	25.8	32	36.0		

As can be noticed from Table 1, more than half (55.6%) of the participants were female (in Slovenia even more than 70%), more than two thirds of them were bachelor students (In Israel more than 80% and in Slovenia only above 30%) and more than 70% of the students in both countries were full time employed students. Regarding the study fields around ¾ were found as affiliated to the social sciences programmes, more precisely from economics more than 40% (what is quite similar in both countries) and from business and management field above 30% (in Slovenia almost 60% and in Israel far less), where the results were as follows: In Israel more than 25% of the students study those subjects and in Slovenia none of those participating in the survey. Therefore, it can be noticed besides the difference in the number of students in Israel and Slovenia, that students who participated in the survey, hold some other differences, that should be taken into account, while discussing the results.

RESULTS

Descriptive analysis was initially conducted to capture the amount of awareness, knowledge and types of behavior toward cyber attacks. The results of the mean and standard deviation scores for the countries total and for each country separately, are presented in Table 2 and Table 3.

The results from the total responders' answers indicted on *medium* awareness to the term "cyber security" (M= 2.44, SD=0.81) similarly, when respondents were asked to indicate the tools from which they enhance their awareness regarding cyber hazard, they pointed to only 4 tools, mostly from internet sources, social media traditional media and talking with friends on average out of 11 listed tools, indicating that the awareness regarding cyber security still needs to be strengthened by them. On the other hand, many of them felt that there are a lot of potential threats in the cyber space (M=4.04, SD=0.87), such as fear from losing data, espionage over people and organization, etc.

Looking at responder's behaviors indicates that they are ambivalent on their behaviors. On the one hand they argue that they know how to behave in the case of a cyber attack (M=3.10, SD=1.19), for example, they indicate that they would not provide information in the web (M=2.42, SD=0.93). In addition, they also argue that their length of a standard password is around 10 in average which is considered by them as safe. However, on the other hand, when we asked the respondents to describe how they act in order to protect their computer, as mentioned before, they only indicated 4 measures on average out of 11 options. They also indicted on less than 2 activities they make when they finish to work on the computer from 4 given options (mostly, log off from all programs and turn off the computer system). More than half of the participants admit that they use the same password for different portals and applications. Such behavior indicates only slight awareness of the need for using real action to protect their devices from cyber attack.

Table 2. Descriptive statistics, mean differences results

Name of a variable	Question / Description	Total	IL	SI	
		Mean (SD)	Mean (SD)	Mean (SD)	T
Awareness	Are you familiar with the term cyber security? (1-no knowledge to 4-very good knowledge)	2.44 (.81)	2.39 (.84)	2.57 (.60)	T= 1.10 p>0.05
Familiarity	Familiarity with different sources? (the variable represents an average of 9 tools)	3.98 (.81)	3.56 (1.91)	4.85 (2.36)	T= 3.83**
IT future	Would like to attend IT security training? (1-definitely not to 5-definitely yes)	3.74 (.97)	3.65 (1.0)	3.97 (.85)	T=1.66 [i]
Threats	The main cyber security threats are? (the variable represents an average score from 14 options)	4.04 (.87)	4.06 (.88)	4.00 (.86)	T= -.35, p>0.05
Effect of education on awareness	The extent to which the current education influenced their cyber-security awareness? (1-definitely not affected to 5-strongly affected)	3.22 (.98)	3.15 (.90)	3.40 (.95)	T=1.29, p>0.05
Provide or find on the Web?	Total sum of the amount of information that the responders provide or find in the Web (1-strongly disagree to 5-strongly agree)	2.42 (.93)	2.54 (.90)	2.13 (.95)	T= -2.19*
Computer skills and knowledge	Self-evaluation of skills and knowledge in using computer application (1-no skills to 5-very high skills)	3.22 (.67)	3.25 (.70)	3.16 (.60)	T=.62, p>0.05
Behavioral	I know how to behave in case of a cyber attack (1-definitely no to 5-rather yes)	3.10 (1.19)	3.07 (1.19)	3.17 (1.20)	T=.66, p>0.05
Choice	Is the use of technology products coming from your desire or by coercion? (1-definitely by coercion to 5-definitely by choice)	3.22 (1.00)	3.40 (.98)	3.11 (1.02)	T=1.46, p>0.05
Protection	Sum of the score in the usage that the responders make to protect their instrument (the variable represent an average of 11 option of procedures that can be used to protect their devices)	4.09 (2.23)	3.50 (1.87)	5.60 (2.39)	T=5.16***
Length	The average length of your standard password (minimum 0 to maximum 14 characters)	9.43 (5.27)	8.99 (5.72)	10.49 (3.85)	T=1.41, p>0.05
Finish	The variable represents an average of 5 processes that can be taken when finishing working of the computer.	1.37 (.73)	1.32 (.67)	1.48 (.88)	T=1.08, p>0.05

Note: [i] p< 0.10; *p<0.05; **p<0.01; ***p<0.005; ****p<0.001

One explanation for the low protection behaviors may result from the participants' previous and existing knowledge. Based on the self-evaluation of skills and knowledge in applications and programs, the results indicated that responders felt they have sufficient knowledge (M=3.32, SD=0.67). They were indifferent toward the motivation to use their technology products either by coercion or desire. Half of them argue that they know the difference between http and https protocol (51.6%). Again, we also found converse results in the responders' answers. Judging their knowledge regarding IT security, only 22% admit they attended an IT security training in the past, but they are willing to participate in this kind of training in the future (M=3.78, SD=0.97). Lastly, respondents argue that the extent to which their current education influenced their cyber security awareness was medium (M=3.22, SD=0.93). Suggesting that while their general knowledge on computers is sufficient, their knowledge regarding IT security is not sufficient at all since it was not being provided to them during their academic education studies.

Differences between Slovenian and Israeli participants

To understand the differences between the Slovenian and Israeli participants, we conducted independent t-test analysis. Slovenian students pointed out more sources from which they knew the concept of cyber security compared to Israeli students (T(122)=3.832, p<0.01). They also applied almost twice more protection measures to protect their instruments compared to Israeli students (T(122)=5.16, p<0.05). Likewise, Israeli students agree to give more information on the web compared to Slovenian students (T(122)=2.19, p<0.05). We found that more than 60% of Israeli students admit that they are using the same password for different portals, systems and

applications compared to 34% of Slovenian students ($X^2(122)=8.31$, $p<0.01$). They also expressed less willingness to participate in IT security cyber courses, compared to Slovenian students and this difference was close to significance ($T(122)=1.66$, $p<0.10$).

Table 3. Percentage of agreement with attendance, recognition and password behaviors statements

Name of a variable	Question / Description	Total[1]	IL[1]	SI[1]	Chi
IT past	Attendance in IT security training in the past?	21.8	23.6	17.1	$X^2=0.647$
Recognition	I usually recognize and know the differences between http and https protocol.	51.6	52.8	48.6	$X^2=0.18$
Password	Do you use the same password for different portals, systems and applications?	54.8	63	34.3	$X^2=8.31$**

Note: [i] p< 0.10; *p<0.05; **p<0.01; ***p<0.005; ****p<0.001
[1]The results indicate the percentage of respondents who agree with the item from the corresponding country

While we did not find significant differences in other variables, the overall image of the differences that were found indicates that Slovenian students not only are more aware of the problem of cyber security than Israeli students, but they also make more effort to avoid cyber hazards. We believe that the difference evolved from the fact that most of Slovenian students were taking the Master courses (69%) while most of the Israeli respondents were BA students (82%). Therefore, student's maturity may be seen as an important factor for the differences in adopting the expected behavior.

DISCUSSION

The current study results reveal that internet users are aware of the term "cyber security". Responders felt that using the internet may expose them to multiple threats either aiming to hurt them or their organization, including violation of their privacy, loss of money or data, damage to their devices, spying on them or their organization, etc. However, we also found a discrepancy between respondent's attitude and their behaviors. Evaluating various types of protection methods reveals that average internet users make basic activities, such as using strong password and installing antivirus software on their computers, so their behavior makes them laymen users. However, only a handful of them perform more sophisticated protection activities that require deep understanding, such as avoiding connecting their computers to unsecured networks (some of the items that go with the attributed protection) and try not to use the same password for different portals and applications (attribute password). Since these activities are not costlier, the reason for that discrepancy is still unknown.

Findings suggested that responders with more knowledge in computer science had expressed a higher positive connection to cyber security awareness. Although being specialized in computer science is not an option available to most of the people, we found that even a partial attendance of a cyber security programme or exposure to cyber security during formal education was positively connected to the amount of awareness to cyber problems.

So, being aware of a problem does not mean that people are taking measures to prevent them from being cyber attacked. Similar to former studies (e.g. Imgraben et al., 2014; Rek & Milanovski, 2017) we found that responders perform basic and not sufficient activities. However, in addition to former studies we also found that some of this discrepancy was connected to their amount of awareness. Higher amount of awareness was positively connected to the number of tools that the responders used to protect their computer from cyber attack, even when controlling the responder's country and gender.

On the other hand, we did not find a connection between the degree of awareness and other tools such as the information from the subjects that agreed to share on the internet or the activities they conducted when finishing working on their computer. As such, when the responders perceived themselves as being able to control the situation by their behaviors, their motivation to take actions increased. Similar to that, we found that responders with more cyber security knowledge execute practical actions in order to prevent their computers and mobile devices from being attacked by cyber malwares, especially when defense tools are simple and familiar to the common internet users.

We also found a connection between the amount of awareness, knowledge and behaviors in the responders' country. These findings could be explained from the culture aspect. Israel is known as a leading technology and cyber country (Tabansky, 2013). Consequently, we assumed that Israeli students do not believe that they should be active in protecting their devices or their organizational assets, since it has already been taken care of by the operator of their device or the organization itself. This is of course not the case in Slovenia, which is not recognized as a leading technology and cyber country, and therefore most of the people know that the protection of their computer against cyber hazards is under their responsibility.

While we found mediation between one type of knowledge, awareness and protection we feel that there are other factors that can be explained in future study, why people do not protect their computes with more means. Based on the theory of planned behavior (Fishbein & Ajzen, 2011), future followed up study can explore how psychological factors, such as self-efficacy as well as the country values (e.g. Hofstede, 2011) effect the internet users behaviors.

CONSLUSIONS

The contributions of this study are as follows:

- It describes and elaborates the existing studies, focusing on what types of cyber hazards exist and what is the internet users attitude towards them. The study provides an initial theoretical framework for cyber awareness, a methodology to evaluate the level of cyber awareness, which could be applied both in academic institutions and schools through face-to-face courses and workshops that supply "targeted" materials for various levels of users according to their IT knowledge and their calculated risk of being victims of cyber hazards. In order to turn the theoretical framework into a practical one, different variables analysed in this study should be taken into account while a new cyber security training course is constructed in order to increase the cyber security awareness among internet users.
- It contributes to the creation of a well-educated society of users with different levels of IT knowledge. It is expected that more funding and effort will be invested in educational programmes and prevention of cyber exploitation in all forms of cyber hazards.
- The importance of cyber awareness education stressed thorough this study may serve as a guide to higher education institutions with the following aspects:
    - When establishing a program for cyber security increase awareness, special care should be given to social humanities students, since we found that within this group of students, the knowledge affiliated with cyber security is lower than the one of more technology oriented ones.
    - In the development and increase in technology usage, the need for tailored programs to enhance the awareness of cyber security knowledge is critical to develop economics and educational systems.
    - The way of building cyber awareness education/training programmes more efficiently is strongly connected to the above two aspects, which should be seriously taken into account by governments and academic institutions, what - among others - Affisco (2017) is arguing.
- Finally, this paper research is based on a comparative study of Israel and Slovenia, which creates an opportunity to learn and benefit from each other on the implication of cyber awareness in higher education and take into account additional factors that contribute to successful implementing efficient cyber security courses and programmes into higher education and therefore lowering the risks of cyber threats as well as improving the cyber knowledge and awareness in the societies of both countries.

REFERENCES

Abawajy, J. (2014), User preferences of cyber security awareness delivery methods. *Behavior & Information Technology*, *33*(3). 236-247.

Affisco, J. F. (2017). Expanding cyber security learning in the business curriculum. P*roceedings for the Northeast Region Decision Sciences Institute* (NEDSI), 420-435.

Benshalom, U., Dvir, A, Levy, Zwilling, M., Orkibi, E., Pele, O. & Gabay, N. (2017). From Internet swear words to stadium violence in football (soccer) games – An Israeli case study, *International Review for the Sociology of Sport* (In press), 1-13. DOI: 10.1177/1012690217715298.

Bong-Hyun, K. & Ki-Chan, K. (2017). Development of Cyber Information Security Education and Training System. *Multimed Tools Appl.*, *76*, 6051-6064.

Dodel, M. & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, *68*, 359-367.

Fishbein, M. & Ajzen, I. (2011). *Predicting and changing behavior: The reasoned action approach.* Psychology Press.

Harris M., & Patten K. (2015). Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum, *Journal of Information Systems Education, 26*(3), 219-234.

Hinduja, S., & Patchin, J. W. (2014). Cyberbullying Identification Prevention, and Response. Cyberbullying Research Center (www.cyberbullying.us). https://cyberbullying.org/ Cyberbullying-Identification-Prevention-Response.pdf

Hofstede, G. (2011). Dimensionalizing cultures: The Hofstede model in context. *Online Readings in Psychology and Culture, 2*(1), 8.

Imgraben J., Engelbrecht A., & Choo K. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users', *Behavior & Information Technology*, 33(12), 1347-1360.

Lukanović L. (2017). "Računalniška kriminaliteta in varstvo osebnih podatkov: diplomska naloga". *Available at: http://www.ediplome.fm-kp.si/Lukanovic_Lea_20171017.pdf*

McCrohan, K., Engel K., & Harvey, J. (2010). Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce*, 9(1), 23-41.

Pawlowski, S., & 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.

Rek, M., & Milanovski, B. K. (2017). Slovenija, Ljubljana: Fakulteta za medije [izdelava], 2016. Slovenija, Ljubljana: Univerza v Ljubljani, Arhiv družboslovnih podatkov [distribucija], IDNo: MPSS16.

Son, J., Bhuse, V., Othmane, L., & Lilien, L. (2015), Incorporating Lab Experience into Computer Security Courses: Three Case Studies. *Global Journal of Enterprise Information System*, *7*(2), 69-80.

Tabansky, L. (2013). Critical Infrastructure Protection Policy: The Israeli Experience. *Journal of Information Warfare*; *12*(3).78-86.