7th International Scientific Conference
Technics and Informatics in Education
Faculty of Technical Sciences, Čačak, Serbia, 25-27th May 2018

Session 2: IT Education and Practice

UDC: 004

An Analysis of User's Information Security Awareness

Đorđe Đurković [1*], Marjan Milošević [2]
[1] Municipal Administration, Ćićevac, Serbia
[2] University of Kragujevac, Faculty of Technical Sciences Čačak, Serbia
[*] djurkovic.djordje93@gmail.com

Abstract: *In modern systems information security is having an increased importance for organizations. With the advance of technology and implementation of guidelines for protecting systems, it is a lot harder for malicious entities to gain access to the system. However one of the main attack vectors is the user, as such it is important for users to be knowledgeable and behave in a way that will have a positive influence in protecting information. Its important for organizations to understand the awareness of users in order to be able to take appropriate actions to increase the safety of the system. This paper is going to do an analysis of user awareness specifically focusing on user's knowledge and behavior. Results of this analysis show us that the current level of user awareness of the Municipal Administration is satisfactory and that age is not important factor for awareness. Information security training is advised, but not necessary.*

Keywords: *Information security, User awareness, information management*

1. INTRODUCTION

The term "information security awareness" is used when it refers to the state in which users in the organization are introduced (ideally dedicated) to their security mission [1]. Information systems are only useful if they are used by people. Similarly, information security awareness is crucial, as information security techniques or procedures can be misused, misinterpreted or not used at all by the user, with that they lose their utility. Increased awareness should minimize user-related errors, in theory it should completely annul them and increase the efficiency of security techniques and procedures from the point of view of users.

Security risks related to information technology are a topic that is getting more and more significant. As corporations are increasingly relying on technology in their business, system security becomes their big concern. In their security report for the last quarter of 2017 Microsoft has reported they observed a 300% increase in the number of attacks on user accounts compared to 2016. Most of these attacks are caused by bad codes or poor password management and are followed by targeted phishing attacks [2].

While information security is mainly focused on the protection of confidentiality, integrity and information accessibility, information security awareness is concerned with the use of programs for security awareness to create and maintain positive behaviors as a critical element in an effective security positive environment. The goal of the information security awareness program is to increase the significance of information systems' protection and reduce possible negative effects of security failures [3]. User security awareness is the degree or level at which each staff member understands the importance of information security, the degree of information security that suits the organization, their individual responsibility of system security and procedures accordingly [4].

Efficient management of information security requires a combination of technical and procedural controls that manage information risk. The value of controls depends on the people implementing and using them and in information security that is no different. Controls can be circumvented or misused from employees who ignore safety rules and procedures. Implementation of effective security control depends on the creation of a security friendly environment, where everyone understands and engages in behaviors that are expected of them. Von Solms R. and Von Solms B. [5] offered guidelines on how to move from information security policy to positive information security culture. The transition to positive information security culture is not always easy and simple, the ISF information security status questionnaire [6] shows that most members think that the effectiveness of their user awareness rising initiative to protect the system is not very effective and four out of five members think they do not invest enough resources and time in this initiative of increasing user awareness.

There seems to be a large number of material to help organizations to form an appropriate program for raising user awareness for information security and how to positively influence the employees. With the following material, organizations can form a good training to raise users information security awareness [7][8][9][10][11].

Consciousness and behavior among all types of users are an important part of the performance of the information security of the organization. Adequate training on information security is essential in the goal of creating and improving user awareness and behavior. Several individual or several combined measures to improve the performance of user information security, they can be distribution of messages via e.g. pamphlets, email, websites, posters, formal presentations, lunch and training sessions. Common to most of these measures is that they are one-way communication directed to a large number of individuals or authorities using expert knowledge. On the other hand, several organizational researchers claim that it is local knowledge through processes that involve employees not only necessary but also efficient in achieving the goal changes in organizational activities [12].

In the past decade research of users' information security awareness was dominantly focused on cognitive behavior. Researchers use multidisciplinary theory, such as theory in psychology, sociology and criminology introduced into models of information security. The most commonly used research theories are Theory of Reasoned Action (TRA) / Theory of Planned behavior (TPB), General Deterrence Theory (GDT), Protection Motivation Theory (PMT), Technology Acceptance Model (TAM) [13].

One of the limitations of applying these theories is that their perspective is of a single level. One theory focuses on individual behavioral factors, despite evidence from different empirical studies that indicate that external factors such as organizational or work factors have influence. Ignoring these factors and their interdependence, theories that explain and predict employee behavior risk being ineffective. The result is that, some researchers have added theoretical extensions of additional factors that affect the individual's behavior, to bridge the gap between individual and external factors in the result of behavior [13].

2. METHODOLOGY

Psychologists suggest that people with learned predispositions respond in a favorable or inconclusive way to a particular object, they have three components: impact, behavior and cognition [14][15]. The impact component involves positive or negative emotions towards something, the components of behavior is the intent of acting in a certain way, while the component of cognition refers to belief and thoughts about an object [14][15].

The methodology for constructing the questionnaire uses the KAB model (knowledge-attitude-behavior) as its basis. This model is based on the theory that if system users have adequate knowledge (information) about the security of the system, they as a result would have a more positive attitude towards the security of the system, the result of which will lead to better behavior [16][17].

Because the aim of this research is to analyze the knowledge and behavior of users in the local government, the compiled survey is exclusively focused on these two aspects.

In the continuation of this paper, a survey of the user awareness of information protection will be done using the survey in the local government of Municipality Ćićevac. During this questionnaire, the main focus will be the next two things:

1. Knowledge of users about the rules of using the computer (system) and basic knowledge of ways of attacking the system through the user.
2. Behavior of users, what procedures users use to facilitate system protection and whether do they have a positive behavior towards information protection.

The survey is mainly based on literature and best practice and consists of 28 questions divided into 2 categories: knowledge and behavior [18][19][20][21]. Users are not aware of these categories and the questions have been distributed so it is not noticeable. All questions carry a certain amount of points, it is possible to achieve a maximum of 100 points, the points are redistributed in such a way that knowledge-related questions carry 50 points and behavior-related questions also carry 50 points.

The first two question are related to: age and years of work experience in the municipality.

Criteria for scoring is focused on the following:

- Knowledge of basic rules of information security
- Understanding the policy put in place for information protection and following it

We have two primary criteria, each of them will yield 2 points. The scoring of the survey itself is done as follows, as there are multiple-answer questions of same importance, the answers were divided in 3 categories: Positive, neutral and negative. A positive answer carries 4 points, neutral 2 points and negative 0 points. Positive answers show that the employee not only has basic knowledge of information security they also understand policies put in place and try to follow them, this is a positive influence on information security as such those answers yield 4 points.

Neutral answer shows that the employee knows basic rules of information security but they don't fully understand the policies put in place and because of that aren't necessarily able to follow them. Those employees don't provide a positive influence but don't necessarily harm information security that is why a neutral answer yields 2 points. Negative answer means that the employee doesn't know the basic rules of information security as such they don't have a positive influence, such answers yield 0 points.

Example of a knowledge-related question with 3 answers:

1. Is the firewall on your computer turned on?
    a. Yes, it is turned on.
    b. No, it is not turned on.
    c. I don't know what a firewall is.

Answer under A is considered a positive response, because the user knows how to check if the firewall is turned on and knows to turn it on. Answer under B is considered a neutral answer because the user knows how to check the firewall but hasn't turned it on. Answer under C is considered a negative one because the user doesn't know what a firewall is.

Example of a behavior-related question with 3 answers:

2. How careful are you during opening attachments that were sent through e-mail?
    a. I always make sure I know the person and that I expect the e-mail.
    b. While I know the company or the person that sent me the e-mail I open the files.
    c. There's nothing wrong with opening files sent via e-mail.

Answer under A is a positive answer because user uses maximum attention during opening of files by making sure he knows who the e-mail is coming from and that he is expecting the e-mail. Answer under B is a neutral one because the user pays some attention during opening of e-mails because he knows he shouldn't open any file that was sent to him especially from someone he doesn't know. Answer under C is a negative answer because the user thinks that there are no negative consequences if he opens files from people he doesn't know so he will not take any precautions.

In table 1 we can see the percentile split of users that participated in this survey.

The largest sample group by age is that of 35-44 years, while the smallest one is the age group of 18-24 years. According to the years of employment the most numerous group is the 6-15 years of employment and the least numerous is 3-5 years. Because of the huge difference in the number of employees by their years of employment, special attention should be paid to the group with 6-15 years of employment because they represent 60% of the participants in this poll.

Table 1. *Sample*

Age	%	Years of employment	%
18-24	6.67	0-2	13.33
25-34	20.00	3-5	6.67
35-44	33.33	6-15	60
45-54	26.67	16-30	6.67
55-64	13.33	31-40	13.33

3. RESULTS

After scoring the survey, users' awareness of information security can be further analyzed. The maximum number of points achievable in the poll is 100, users have on average achieved 65.37 points. With this information the average user awareness of information security can be concluded. As shown in Chart 1. The average user is aware (knowledge and behavior) of 65.37% procedures that are meant to relieve system security and is not aware about 34.63% of them.

Figure 1. *User awareness by percentage*

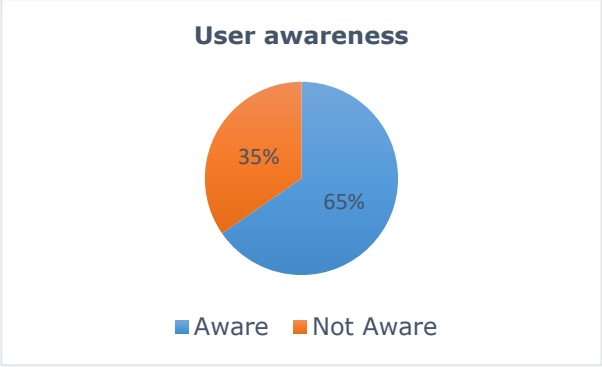

Table 2. *User awareness by age*

Age	Points	Knowledge	Behavior	Knowledge %	Behavior %
18-24	92.00	44.00	48.00	47.83	52.17
25-34	72.67	32.67	40.00	44.95	55.05
35-44	63.67	25.33	38.33	39.79	60.21
45-54	64.50	26.50	38.00	41.09	58.91
55-65	48.00	17.00	31.00	35.42	64.58
Average	68.17	29.10	39.07	41.81	58.19

Age categories are 18-24, 25-34, 35-44, 45-54 and 55-64 for each category an average amount of points the employees achieved in the survey is calculated. This is further divided into the amount of points the employees achieved in knowledge and behavior as well as their average. In addition, the percentage of points the users achieved in

knowledge and behavior is calculated for each age group as well as their average.

As it can be seen in table 2, 3 age categories (35 to 65) are below the average awareness of users, the most aware are employees in the age group 18-34 years old and highly aware are employees in the age group 18-24 with average of 92 points. According to the results from table 2 it can be clearly seen that the age group of 18-24 years old with the average points of 44 in knowledge has the highest average, compared with the age group of 55-65 has only 17 points on average.

In order to find out if there is significant difference among workers in terms of age, two groups are formed: one's age is below 45, and the other is 45 and above. The ANOVA analysis is applied for the behavior test-results and for the knowledge-test result. Idea is to find out if the null hypothesis can be proved, that is to find out if the age is important for security awareness.

ANOVA analysis results are presented in Tables 3 and 4.

Table 3. *ANOVA analysis on behavior*

SUMMARY						
Groups	**Count**	**Sum**	**Average**	**Variance**		
Junior	10	398	39.8	51.06667		
Senior	6	214	35.66667	47.06667		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	64.06667	1	64.06667	1.290675	0.274998	4.60011
Within Groups	694.9333	14	49.6381			
Total	759	15				

Table 4. *ANOVA analysis on knowledge*

SUMMARY						
Groups	**Count**	**Sum**	**Average**	**Variance**		
Junior	10	294	29.4	97.82222		
Senior	6	130	21.66667	77.46667		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	224.2667	1	224.2667	2.476651	0.137869	4.60011
Within Groups	1267.733	14	90.55238			
Total	1492	15				

Since F_{crit} in both cases is greater than F, it can be concluded that there is no significant difference between groups and therefore the null hypothesis cannot be rejected. That means that age category cannot be taken as important for security awareness.

4. CONCLUSION

Serbian government is comprehensively digitizing its services because of the sensitivity of data a government body handles; it is becoming more important for the employees to be aware of possible threats to information security. As such there needs to be a level of awareness required to be obtained and maintained by every employee. The boundary of an aware employee and a non-aware one would be considered achieving enough points on this survey to get a passing grade in a University as such we will consider those employees who have achieved over 50% to be aware and a positive influence on information security. An aware employee knows, understands and takes necessary steps to uphold a positive information security environment. According to the results of the analysis we see that users average 65.37 points in the survey, this level of

information security awareness is satisfactory. The sample is very small to draw solid conclusions. Although youngest employees and those who are recently employed got more points than other age subcategories, no statistical evidence was found that there is a strong connection between age and awareness. Still, forming and holding an adequate training on raising users information security awareness would help not only users to gain knowledge about ways they can protect the system, but would further improve the already existing positive behavior of users towards information security. Because of the intensive modernization of local governments in Serbia, if this modernization is not accompanied by detailed and appropriate training, there will be situations where the lack of knowledge of users will have a negative effect on information security behavior.

ACKNOWLEDGEMENTS

This work is partly supported by Ministry of Education, Science and Technological Development through project III47003, Infrastructure for electronic supported learning in Serbia.

REFERENCES

[1] M. Siponen, "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*, vol. 8, no. 1, pp. 31-41, 2000.

[2] "Global Security Intelligence Report | Microsoft", *Microsoft Security - US (English)*, 2018. [Online]. Available: https://www.microsoft.com/en-us/security/intelligence-report,[Accessed:01- Apr- 2018].

[3] S. Hansche, "Designing a Security Awareness Program: Part 1", *Information Systems Security*, vol. 9, no. 6, pp. 1-9, 2001.

[4] ISF, "The Standard of good practice for information security". *Information Security forum*, 2016.

[5] R. von Solms and B. von Solms, "From policies to culture", *Computers & Security*, vol. 23, no. 4, pp. 275-279, 2004.

[6] ISF, "Effective security awareness – workshop report"*, Information security, 2002.*

[7] ISF, "The standard of good practice for information security*", Version 4.0,* Information security forum, 2003.

[8] ISO/IEC 27002, "Information technology, security techniques"*, Code of practice for information security controls, 2013.*

[9] J. Leach, "Improving user security behaviour", *Computers & Security*, vol. 22, no. 8, pp. 685-692, 2003.

[10] A. Martins and J. Elofe, "Information Security Culture", IFIP *Advances in Information and Communication Technology*, pp. 203-214, 2002.

[11] P. Spurling, "Promoting security awareness and commitment", *Information Management & Computer Security*, vol. 3, no. 2, pp. 20-26, 1995.

[12] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers & Security*, vol. 29, no. 4, pp. 432-445, 2010.

[13] B. Lebek, J. Uffen, M. Breitner, M. Neumann and B. Hohler, "Employees' Information Security Awareness and Behavior: A Literature Review", 2013 46th *Hawaii International Conference on System* Sciences, 2013.

[14] R. Feldman, Understanding psychology. New York, NY: McGraw-Hill, 2013.

[15] H. Michener and J. DeLamater, *Social psychology*. Forth Worth: Harcourt Brace College Publishers, 1994.

[16] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius and C. Jerram, "A study of information security awareness in Australian government organisations", *Information Management & Computer Security*, vol. 22, no. 4, pp. 334-345, 2014.

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

[18] *SANS, "Security Awareness Survey", 2012,* https://www.sans.org/sites/default/files/2018-01/security-awareness-survey.pdf (Accessed in May 1. 2018)

[19] University of Louisville, "Survey on the Internet Security Awareness", 2009, https://www.kansai-u.ac.jp/riss/en/shareduse/data/17_E_questionnaire.pdf (Accessed on May 1. 2018.)

[20] *SAI global, "Information Security Awareness survey", 2008,* https://www.saiglobal.com/compliance/resources/whitepapers/information-security-awareness-survey-results.pdf (Accessed On May 1. 2018.)

[21] *The University of Warwick,* "Information security Awareness Questionnaire", https://warwick.ac.uk/services/idc/informationsecurity/questionnaire/ (Accessed on May 1. 2018.)