ISSN 1846-6168 (Print), ISSN 1848-5588 (Online)
https://doi.org/10.31803/tg-20180717222848

Preliminary communication

INFORMATION SECURITY: THREAT FROM EMPLOYEES

Aleksandar ERCEG

Abstract: Information security inside the organization is becoming a major issue in the modern and global world. Information accessibility and security are a major issue where user behaviour plays an important role. Information security user behaviour is becoming an increasing threat to their organization information security. Since the organization is investing in and implementing information security systems, the issue of employees' behaviour has become increasingly important. This paper aims to show how workers treat information security and is looking upon so called "people problem". In the research, the personal behaviour of health care professionals and workers in a Croatian production company in relation to information security was tested. Results have shown that the overall behaviour of respondents in production company is more responsible and security awareness with proper use of passwords is associated with knowledge about the importance of security application in their work. Further research is recommended.

Keywords: business data; healthcare; information security; passwords; production company; security risk

1 INTRODUCTION

Information security involves people and technology. Up to 90% of companies and organizations encounter at least one information security incident during the business year [1]. In the last several years, there has been a significantly rising concern about information security and behaviour of people which is simply described by Schneier [2, p. 256] who stated to "tell prospective clients that the mathematics are impeccable, the computers are evincible, the networks are lousy, and the people are abysmal. I have learned a lot about the problems of securing computers and networks, but none that really helps solve the people problem."

Stanton et. al. [3] stated that although organizations tend to be concerned about external threats, the recent situation is showing that a substantial part of incidents is coming from inside of the organization. Today many believe that promotion of end user good behaviour is important to model for effective information security policies inside organizations. End user and their information security related behaviour can influence a total information security and therefore they can be of great benefit for managers, information technologists and others connected to assessing and/or influencing end user behaviour.

In this paper, the so called "people problem" will be examined and how employees threat potential information risks by sharing their passwords, making backups, etc., and how this can influence organization information security. The paper is divided into several parts. In the first part, the literature overview is given. In the second, the methodology is presented followed by data analysis and a discussion section where findings are shown. The last part contains the brief conclusion of the paper and implications for further research are provided.

2 INFORMATION SECURITY

Information is the most valuable asset an organization (private, public, government, nongovernment) can have. Therefore, it is of utmost importance to develop a combination of systems, operation and internal procedures for ensuring the integrity and secrecy of data and operational procedures in the organization [4]. Benefits of computerization are numerous both in health and in the business sector. The development of communication networks in the global communications area has destroyed all classic protection systems of information and communication, ranging from the protection system from the so-called "viruses" to unauthorized access to information. Information security is influenced by the environment in which information is exchanged and communicated. The rapid development of information and communication technology has further increased the complexity of the security environment over the past two decades [5]. Information security represents the protection of information systems and information from potential unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Thus, the information security becomes part of our lives. Information security is influenced by the people who use them and the same technologies that enable these processes in accordance with which it takes place. The increasing influence of thinking about information security policies indicates the width and complexity of the content that is being covered. Information security can be defined as a state of condition of confidentiality, integrity, and availability of data, which is achieved by applying certain standards and measures, and organizational support for business planning, implementation, verification, and updating of standards and measures [6]. The aim of information security activities is the detection and prevention of non-authorized information technology user activities [7]. Chang and Lin [8, p. 7] stated that information security is a social and organizational problem since technical systems must be operated and used by people.

Information and communication technologies users can significantly affect the information system security [9] and are still considered the weakest link of information security [8], [10]. A significant influence on the development of information security policies has additional factors that so far have not been considered, such as the structure of the organization and its culture [5]. Kaushal and Khan [10] proposed an information security life cycle. (Fig. 1)

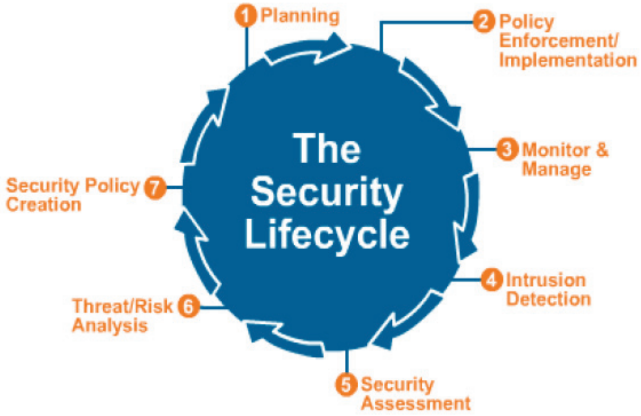


Figure 1 Information security life cycle [10, p. 123]

The previous figure presents information security life cycle with several important phases and it is necessary for successful management of information security programs. Every step shows the importance of the approach to information security. It is of utmost significance for the organization to recognize that this process is never-ending, and that organization needs to improve its behaviour during every cycle.

Information security is needed because the technology applied to information creates risks. In cases when information security risk is recognized and is stable, it is necessary to create a policy for information security. These policies can be divided into four categories: protection measures, detection measures, consequences response measures and measures to ensure the effectiveness of the consequences response.

3 LITERATURE OVERVIEW

In the previous ten years, research in the field of security technology has been increased. Most of these studies were focused on the impact of human factors and questions the usefulness of security mechanisms in information and communication technologies. Previous studies [11], [12] investigated the impact of human behaviour on information security in companies. Their results, among other things, pointed out the everyday behaviour of employees in relation to the use of information and communication technologies and the possibility of preventive behaviours to avoid problems. Research conducted in Germany [13] indicated that security measures whose aim is information security are necessary. These measures should be designed to address the key risks and their consequences. While organizations today rely significantly on information technology and information security is of increasing attention, today there are only a few strategies for information security practitioners [4].

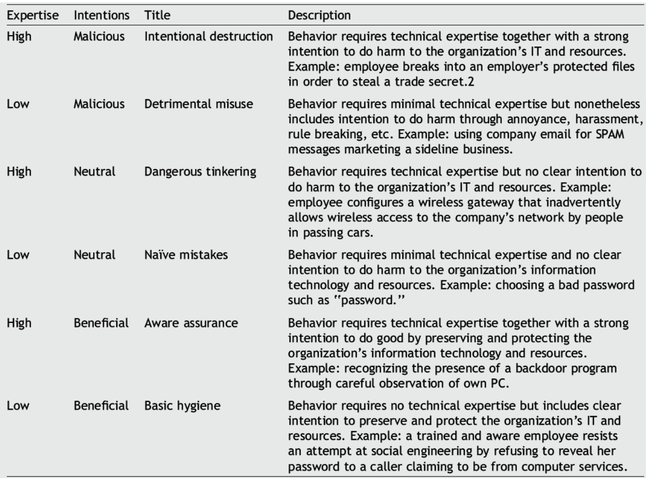
Due to the increasing need for data protection that is mostly present and developed in the banking and financial sector, management of companies is increasingly considering information security management as their direct responsibility and that because of information security ignorance significant personal, financial and legal responsibility can occur. It is important to state that Gaunt [14] proposed information security awareness programs for improving information security behaviour in healthcare contexts. For this reason, we should not neglect the role of the user that can affect the level of system security with its risk behaviour [9] – according to statistical data it is proved that most of the security breaches in business organizations are caused unintentionally [15]. Therefore, the information security and its management have become an important business responsibility of the top-level company's management boards [16]. Almost 75% of big corporations have suffered security breaches because of staff related activities and 50% of the worst breaches were caused by human error [17]. Those security breaches were the result of unwitting security compromises.

The most common form of business communication is e-mail, with the recommendation of using a business address that is controlled by the institution and where all security requirements are met. According to Cyber security survey in 2017, more than 70% of security breaches were the result of staff receiving the fraudulent e-mail. The survey revealed that only 20% of staff attended information security training [18].

In addition to the e-mail communication security, it is necessary to reduce medical data security vulnerabilities, which may have a negative impact on health care data protection [19]. Research about the role of users related to information security is still rare, while previous studies usually focus on the password as the first line of defence in most information systems. Studies have shown that despite the recommendations on the password selection, users still tend to select those passwords that are simple and easy to remember or those concerning their personal data [20]. Despite the training, users still have the habit to share their passwords with their colleagues, write them in a visible place, or do not change them for a long time, which confirms that the user behaviour is a very common problem in the field of security and that education is still necessary [21]. Different techniques for estimation of user's risk behaviour have been developed, and one of the latest is the algorithm for evidential reasoning that is used to assess and compare the status of multiple systems [9].

But it seems that the awareness among users about the importance of the health care system (which in Croatia is the public service) may be worse in relation to the average user in the business sector. Although financial damage can be large-scale, security incidents with data from the electronic health record can cause long-term much higher, even material, damage to the individual person. Similar previous research on the awareness of ICT users in terms of safety and their behaviour are very scared and particularly on the issue of health care professionals.

Several researchers started with the development of different concepts and theories relevant to the influence of user behaviour to organization information security. Among them, Stanton et al. [3] in their research catalogued and analysed a range of end user security behaviour in organizations (Fig. 2).



Expertise	Intentions	Title	Description
High	Malicious	Intentional destruction	Behavior requires technical expertise together with a strong intention to do harm to the organization's IT and resources. Example: employee breaks into an employer's protected files in order to steal a trade secret.2
Low	Malicious	Detrimental misuse	Behavior requires minimal technical expertise but nonetheless includes intention to do harm through annoyance, harassment, rule breaking, etc. Example: using company email for SPAM messages marketing a sideline business.
High	Neutral	Dangerous tinkering	Behavior requires technical expertise but no clear intention to do harm to the organization's IT and resources. Example: employee configures a wireless gateway that inadvertently allows wireless access to the company's network by people in passing cars.
Low	Neutral	Naïve mistakes	Behavior requires minimal technical expertise and no clear intention to do harm to the organization's information technology and resources. Example: choosing a bad password such as "password."
High	Beneficial	Aware assurance	Behavior requires technical expertise together with a strong intention to do good by preserving and protecting the organization's information technology and resources. Example: recognizing the presence of a backdoor program through careful observation of own PC.
Low	Beneficial	Basic hygiene	Behavior requires no technical expertise but includes clear intention to preserve and protect the organization's IT and resources. Example: a trained and aware employee resists an attempt at social engineering by refusing to reveal her password to a caller claiming to be from computer services.

Figure 2 Two factors taxonomy of security behaviour [21, p. 126]

The previous figure shows categories of possible user security behaviour in organizations that are arranged in two dimensions. This taxonomy can help with tasks in examining and controlling user information security behaviour in organizations. Siponen et al. [22] in their research confirm that major threats to information security are careless employees and they not only have to be aware of information security policies and procedures but also must comply with them. To influence information security related behaviour top management and information security staff should clearly state the importance of complying with organization information security policy. Ajzen [23] found that the intention to comply with information security policies can significantly impact behaviour; the stronger an intention to engage in behaviour is, it is more likely to be performed.

4 MATERIAL AND METHODS

The aim of this research was to determine whether there were differences in user information security behaviour among health care workers and workers in the private company situated in the same Croatian town.

The research was conducted by a certified survey of risk behaviour - Users' Information Security Awareness Questionnaire (UISAQ) which measures the level of information system's users' awareness on security matters, as general as possible. The UISAQ questionnaire has two main scales and six subscales: Potentially Risky Behaviour, Usual Behaviour, Personal Computer Maintenance, Borrowing Accessing Data, Knowledge and Awareness, Security in Communications, Secured Data, Backup Quality. These subscales describe user's behaviour, knowledge, and awareness [24].

UISAQ allows IT professionals' better analyses of information systems users and it helps them in identifying issues with the low security level. On the other side, UISAQ can help researchers in the better categorization of users in relation to their security awareness. This tool can be helpful in gaining a conclusion about user's risky behaviour, making correlations with security awareness level and potential identification of unsecure users.

A survey in this paper was used to determine user impact on the overall system security in hospital and in private company. The study was conducted on 152 respondents, of whom 88 (57.9%) were health care professionals (nurses/technicians, physicians) employed in Healthcare institution (hospital respondents) and 64 (42.1%) of respondents were employed in a Croatian production company (private company respondents).

5 RESULTS AND DISCUSSION

The average age of respondents working in hospital was 40 (IQR 30 – 48) years, without significant differences in relation to respondents from production company whose average age iwass 43 years (37 – 47). Women are more represented in the hospital (Fisher's exact test, $p = 0.003$), and there are significantly more employees with university degrees employed in production company (χ^2 test, $p < 0.001$). According to the educational program a total of 66 (43.7%) respondents completed graduate study, more are non-hospital employees (Fisher's exact test, $p < 0.001$). Although in both institutions in a time of employment, employees, when given username and password, signed the rules they need to comply, only 82 (55%) of respondents recalled having signed the document, significantly more from production company (Fisher's exact test, $p < 0.001$). When asked to write their password for analyses and assessment of the password quality, as many as 79 (52%) respondents wrote theirs, significantly more from production company (Fisher exact test, $p < 0,001$). Although production company employees have written their "passwords", it was impossible to check if the passwords were true. (Tab. 1)

Table 1 Groups scale mean scores

	Number of respondents (5)			p*
	Hospital	Private company	Total	
Gender				
Men	22.7	46.9	32.9	0.003
Women	77.3	53.1	67.1	
Education level				
High School	39.8	15.9	29.8	<0.001
College	28.4	11.1	21.2	
University	31.8	73	49	
Working place				
Higher management	0	3.1	1.3	0.222
Middle management	25.3	28.1	26.5	
Employee	74.7	68.8	72.2	
Educational program				
High school	39.8	15.9	29.8	<0.001
Professional study	18.2	9.5	14.6	
Undergraduate study	9.1	0	5.3	
Graduate study	27.3	66.7	43.7	
Post-graduate study	5.7	7.9	6.6	
Signed the rules for using the institution information system	40.5	75	55.4	<0.001
On the survey typed their password	38.6	70.3	52	<0.001

Respondent's behaviour was rated over 17 questions in three areas: lending, behaviour, and confidence. Sometimes 15 (9.9%) respondents lend official access data (username and password) to fellow work colleagues, who find themselves in need. Different passwords for different systems are always used by 35 (23.3%) respondents (i.e. for Facebook one, for e-mail another, for business system third password, etc.), 48 of respondents (32%) never used more than one e-mail address (i.e. private and official e-mail), and 97 (63.8%) never locked business computer during brief departure from the office, classroom, working place. 90 (59.6%) respondents never install various programs of unknown and less known manufacturers, which may be interesting but not necessary for work (i.e. different video players, multimedia accessories, web browsers). On social networks, 25 (16.4%) of respondents rarely leave personal information (i.e. private address, cell phone number, the message that they are on holiday, etc.). (Fig. 3)

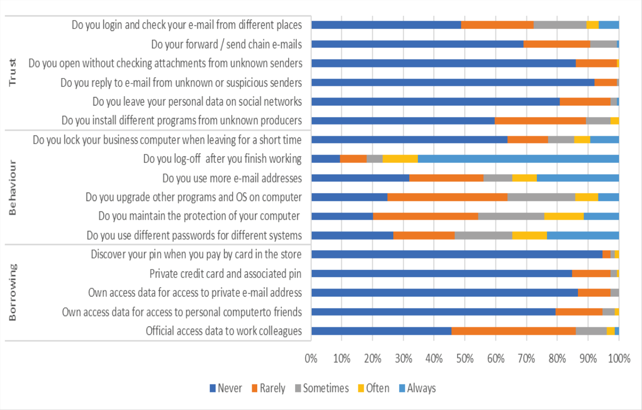


Figure 3 Respondents according to the behaviour scale

Communication over social networks is considered as totally insecure by 47 (30.9%) respondents, and 64 (42.1%) respondents stated mobile phone communication as quite insecure (talking and SMS). Correspondence over e-mail is considered quite insecure by 43 (28.3%) respondents. (Fig. 4)

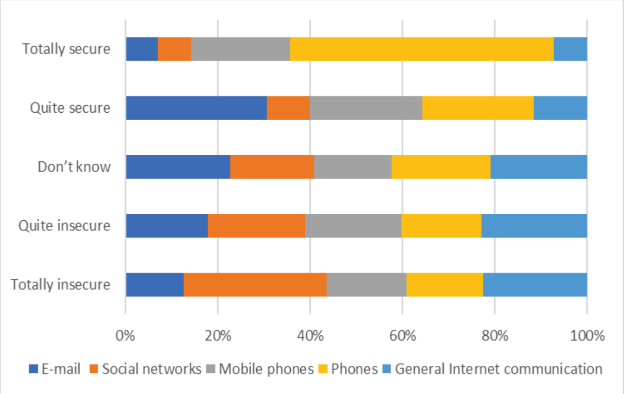


Figure 4 The distribution of answers according to the security level

According to the belief level, most respondents 59 (39.3%) are not convinced that someone will take money from their bank account, while 19 (12.6%) are convinced that someone will steal their identity on the internet (e-mail, e-banking, Facebook, etc.). (Fig. 5)

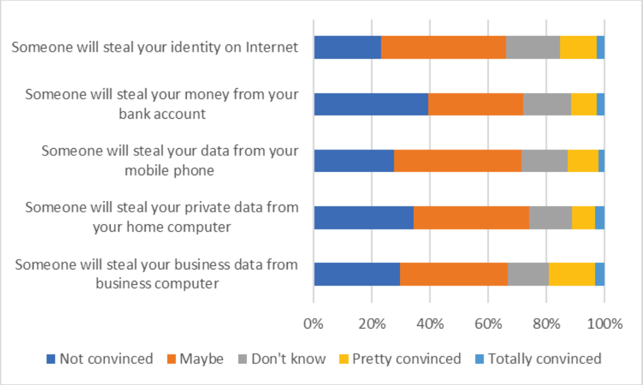


Figure 5 The distribution of answers according to the belief level

Unconditionally maintenance of their passwords is totally unimportant for 13 (8.6%) respondents and extremely important 66 (43.7%) respondents. Periodical replacement of their passwords with new ones, at least for important systems is quite important for 73 (48.3%) respondents, and 72 (47.7%) respondents stated that is extremely important to separate business from private computing resources (i.e. USB memory, e-mail, phone). (Fig. 6)

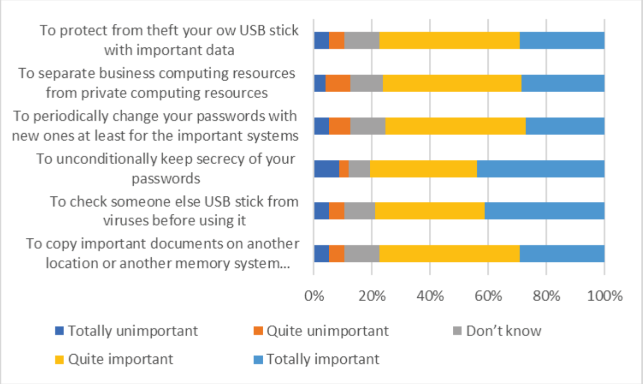


Figure 6 The distribution of answers according to the importance level

Behaviour scale means score 2 (interquartile range 1.8 – 2.2) is significantly worse with hospital respondents (Mann Whitney test, p = 0.038). Significant are differences in behaviour subscale where respondents from production company are acting as more responsible (Mann Whitney test, p = 0.011), with scale mean score 3 (interquartile range 2.3 – 3.6). With security and importance scale there is no significant difference between the mean scale score between the two groups. Belief scale mean score of 4 (3.3 – 4.4), is significantly higher with production company employees (Mann Whitney test, p = 0.027). (Tab. 2)

Personal data security has been determined by the time when the last backups of personal data and documents have been made and with the number of persons that know the respondent's password. Out of survey respondents, 28 of them (18.55%), of which 10 (11.5%) from hospital and 18 (28.1%) from production company, never made a backup of their documents. 30 (20%) participants stated that besides them two more people knew their password, of whom significantly more, 17 (26.6%), from the production company. 26 (30.2%) participants from hospital stated that they were the only ones who knew their password, which is significantly less in relation to the participants from production company (Fisher exact test, *p* = 0.020). While comparing personal data security with those respondents who wrote their password in the survey there is significantly more respondents from production company – 20 (44.4%) and at the same time, they stated that they were the only ones that knew their password (Fisher exact test, *p* = 0.046). (Tab. 3)

Table 2 Groups scale mean scores

Mean rating	Median (interquartile range)			*p**
	Hospital respondents	Private company	Total	
Behaviour scale	2.2	2.0	2.0	0.038
Borrowing	1.2.	1.2	1.2	0.988
Behaviour	3.3	3	3.2	0.011
Trust	1.2	1.3	1.3	0.078
Security scale	2.2	2.4	2.2	0.393
Belief scale	4	4.2	4	0.027
Importance scale	1.8	1.8	1.8	0.811

Table 3 Respondents according to answers about data security and groups

Personal data security	Number of respondents (%)			*p**
	Hospital respondents	Company respondents	Total	
When was the last time the backup of personal data and documents made?				
Never	11,5	28.1	18.5	0.053
Don't' remember	43.7	32.8	39.1	
During last six months	23	26.6	24.5	
During last month	17.2	7.8	13.2	
Last week	4.6	4.7	4.6	
How many people know respondent's password for accessing e-mail system?				
More than 10	8.1	0	4.7	0.020
From 5 to 10	7	7.8	7.3	
Me and two more	15.1	26.6	20	
Me and one more	39.5	25	33.3	
Only me	30.2	40.6	34.7	
When did you make a backup of personal files and documents last time?				
Never	5.9	28.9	19	0.058
Don't remember	44.1	24.4	32.9	
During the last six months	29.4	33.3	31.6	
During last month	14.7	8.9	11.4	
Last week	5.9	4.4	5.1	
How many people know the password for accessing your own e-mail?				
More than 10	2.9	0	1.3	0.046
From 5 to 10	0	8.9	5.1	
Me and two more	20.6	26.7	24.1	
Me and one more	44.1	20	30.4	
Only me	32.4	44.4	39.2	

Through the research, it has been shown that the overall behaviour of respondents in production company (*p* = 0.011) is more responsible, which confirms previous research on the use of e-mail addresses according to which the respondents from technical scientific fields use more secure official e-mail addresses, as opposed to biomedical researchers. Different passwords for different systems are used by 23.3% of respondents, which is slightly less than it was found in research on 836 subjects [25], of whom 31% always use different passwords. The introduction of "single sign-on" (SSO) i.e. single logging into the system, which institutions began to implement [26], would reduce the burden on employees about remembering multiple passwords. Analyses [27] showed that the awareness of users toward to the information system security and proper use of passwords is associated with knowledge about the importance of security application in their work. The ratio of respondents to the question of personal data security proved to be very weak - 18.5% of respondents had never made a backup of their data, and 39.1% could not remember when they had done it the last time, where the distribution frequency of making backups among medical and electrical engineering students is very low.

Among all respondents, 28, of whom 10 (12%) are from the hospital and 18 (28%) are from the production company, have never made a copy of their documents. To question about password sharing, 30 (20%) respondents stated that two more people knew their password, of which significantly more, 17 (27%) from production company, while 26 (30%) of hospital respondents stated that they didn't share their password, which is significantly less than those not working in hospital (Fisher's exact test, *p* = 0.020). Comparing the security of personal data from those respondents who wrote their password in questionnaire there are significantly more respondents from production company - 20 of them (44%), while at the same time they claim that they are the only one which knows their password (Fisher's exact test, *p* = 0.046).

5 FINAL REMARKS AND CONCLUSION

Most research agrees that almost highest threat to an organization's information security comes from employees who do not follow set information security procedures. Employees must be aware of and follow information policies and procedures. Entire company (hospital, government, private) plays important role in presenting policies and procedures for user information security behaviour. Education of employees should be a major task in today's information era where everything is available to everyone; also, information must be treated as secure as possible when it is necessary.

Although user information security behaviour in different industrial sectors was compared in the research, there are similarities in the user behaviour. In both examined companies there are users that care about information security but also many of them do not think that information security is important for a company's efficiency. Research results have shown that employees in a private company behave better in relation to information security. They are more responsible and security aware regarding password usage and have better knowledge about the importance of security application in their work.

To conclude, it is appropriate to propose further research on information security behaviour and to check relation between different production companies in Croatia and their approach in solving so called "people problem" in dealing with information security since it was found in research that although employees signed a statement about information security, not many of them remembered it and some of them did not comply with it.

6 REFERENCES

[1] Bagchi, K. &, Udo, G. (2003). An analysis of the growth of computer and Internet security breaches. *Communications of AIS*, 2, 684-700. https://doi.org/10.17705/1CAIS.01246

[2] Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley & Sons, Inc.

[3] Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviours. *Computers & Security, 24*(2), 124-133. https://doi.org/10.1016/j.cose.2004.07.001

[4] Hon, K., Chi, Y., Chao, L. P., & Tang, J. (2003). An integrated system theory of information security management. *Information Management and Computer Security, 11*(5), 243-248. https://doi.org/10.1108/09685220310500153

[5] http://www.fer.unizg.hr/download/repository/Kvalifika-cijskiDrIspit_AK_08022010.pdf (Accessed on April 2018)

[6] Narodne novine. (2007). Zakon o tajnosti podataka i informacijskoj sigurnosti (in Croatian).

[7] Gollmann, D. (1999). *Computer Security*, New York: John Wiley & Sons.

[8] Chang, S. E. & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458. https://doi.org/10.1108/02635570710734316

[9] Šolić, K., Jović, F., & Blažević, D. (2013). An Approach to The Assessment of Potentially Risky Behaviour of ICT System's Users, *Technical Gazette*, 20(2), 335-342.

[10] Kaushal, P. & Khan, R. (2018). A Review on Information Security. *International Journal of Advanced Research in Computer Science and Software Engineering, 8*(4), 122-124. https://doi.org/10.23956/ijarcsse.v8i4.646

[11] Bisset, J. K. & Shipton, G. (2000). Some Human Dimensions of computer virus creation and infection. *International Journal of Human-Computer Studies, 52*(5), 899-913. https://doi.org/10.1006/ijhc.1999.0361

[12] Marioani, M. G. & Zappala, S. (2014). PC Virus attacks in small firms: Effects of risks perceptions and information technology competence on preventive behaviours. *TPM, 21*(1), 51-65.

[13] https://www.dcsec.uni-hannover.de/uploads/tx_ tkpublikationen/risk-survey-csf.pdf (Accessed on April 2018)

[14] Gaunt, N. (1998). Installing an appropriate information security policy in hospitals. *International Journal of Medical Informatics, 49*(1), 131-134. https://doi.org/10.1016/S1386-5056(98)00022-7

[15] https://www.bsi.bund.de/SharedDocs/Downloads/EN/ BSI/Grundschutz/guidelines/IT-sec-guidelines_pdf.pdf?__ blob=publicationFile (Accessed on March 2018)

[16] Von Solms, B. & Von Solms, R. (2005). From information to... business security? *Computer & Security, 24*(4), 271-273. https://doi.org/10.1016/j.cose.2005.04.004

[17] https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf, (Accessed May 2018)

[18] https://assets.publishing.service.gov.uk/government/up-loads/ system/uploads/attachment_data/file/609186/Cyber_Security_ Breaches_Survey_2017_main_report_PUBLIC.pdf (Accessed May 2018)

[19] Dantu, R., Oosterwijk, H., Kolan, P., & Husna, H. (2007). Securing medical networks. *Network Security, 2007*(6), 13-16. https://doi.org/10.1016/S1353-4858(07)70055-7

[20] Taneski, V., Heričko, M., & Brumen, B. (2014). Password security – no change in 35 years? *Proceedings of 37th International Convention Information and Communication Technology, Electronics and Microelectronics*, Opatija, 1360-1365. https://doi.org/10.1109/MIPRO.2014.6859779

[21] Sedinić, I., Lovrić, Z., & Perušić, T. (2014). Costumer and User education as a tool to increase security level. *Proceedings of 37th International Convention Information and Communication Technology, Electronics and Microelectronics* Opatija, 1441-1445. https://doi.org/10.1109/MIPRO.2014.6859793

[22] Siponen, M., Pahnila, S. & Mahmood, A. (2014). Employees' Adherence to Information Security Policies: An Empirical Study. *Information & Management, 51*(2), 217-22. https://doi.org/10.1016/j.im.2013.08.006

[23] Ajzen, I. (1991). The Theory of Planned Behaviour. *Organizational Behaviour and Human Decision Processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

[24] Šolić, K., Velki, T., & Galba, T. (2015) Empirical study on ICT system's users' risky behaviour and security awareness. *Proceedings of 38th International Convention Information and Communication Technology, Electronics and Microelectronics*, Opatija, 1623-1626. https://doi.org/10.1109/MIPRO.2015.7160485

[25] Hoonakker, P., Bornoe, N., & Carayon, P. (2009). Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, San Antonio, 53(6), 459-463. https://doi.org/10.1177/154193120905300605

[26] Sasse, M. A., Brostoffand, S., & Weirich, D. (2001). Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19, 122-131. https://doi.org/10.1023/A:1011902718709

[27] Duggan, G. B., Johnson, H., & Grawemeyer, B. (2012). Rational Security: Modelling Everyday Password Use. *International Journal Human Computer Studies, 70*(6), 415-431. https://doi.org/10.1016/j.ijhcs.2012.02.008

Author's contacts:

Aleksandar ERCEG, Ph.D., Assistant Professor
J. J. Strossmayer University of Osijek,
Faculty of Economics in Osijek,
Trg Ljudevita Gaja 7, 31 000 Osijek, Croatia
aleksandar.erceg@efos.hr