Human aspects of information security questionnaire (HAIS-Q) – Croatian translation and validation

Suzana Prenđa (suzana.prendja@gmail.com)
Ministry of Defense, Croatia

Petra Mikac (petrammartincic@gmail.com)
Ministry of Defense, Croatia

Suzana Rački (suzana.racki@ gmail.com)
Ministry of Defense, Croatia

Abstract

The most vulnerable aspect of the information security system is the human factor. Therefore, information security awareness (ISA) among employees is the key to mitigating risk and protecting organizations from social engineering and cyber attacks. The aim of this research was to adapt and validate the Human Aspects of Information Security Questionnaire (HAIS-Q) on the Croatian population to get a fast, cost-efficient, comprehensive, work behavior-oriented ISA assessment method. The HAIS-Q based on the knowledge-attitudes-behavior model (KAB) was taken for that purpose. Each assessment area in HAIS-Q (knowledge, attitudes and behavior) consists of seven focus areas which represent specific areas of human aspects of IS. The validation of the questionnaire was carried out in three phases. In the first phase, the questionnaire was translated and adapted in collaboration with psychologists, translators and experts in IS. In the second phase, a pilot study was conducted on 18 participants, and some items were simplified and certain terms changed. In the third phase, the main study was conducted to further check the validity, reliability and sensitivity of the questionnaire. All of those parameters were found satisfactory. The responses on individual items are distributed in the full range of possible responses, which shows good sensitivity. Cronbach's Alpha coefficients indicate that the scales measure the same construct, which shows high reliability. Pearson correlation coefficients that show correlation between the HAIS-Q results and risk behavior assessments, as well as between the HAIS-Q results and the Users' Information Security Awareness Questionnaire (UISAQ) results, indicate good validity. Therefore, the results indicate that the questionnaire can be used for a simple and quick assessment of ISA and as a basis for improving IS. The collected data enable an overview of the greatest risks of IS within the framework of human aspects in an organization, which can be used for education, improvement of existing security measures of the organization or development of new ones. Shortcomings and recommendations for further development are listed.

Keywords: *Information Security Awareness; HAIS-Q; Knowledge-Attitudes-Behavior model, UISAQ; Croatian; translation; validation; work behavior-oriented questionnaire*

Introduction

Information security (IS) is defined as "the state of confidentiality, integrity and availability of data" (Information Security Act, NN 79/2007-2484). In addition to technical protection measures (firewall, antivirus program, encryption, etc.), it is clear that IS is largely influenced by the human factor (Arbanas, 2020). Humans are often referred to in the literature as the "weakest link in the security

chain", as they are the most common cause of security breaches (Furnell and Clarke, 2012; Mahfuth et al., 2017; Yoo et al., 2019). However, this also makes them the "first line of defense" when it comes to protecting IS. The degree to which an organization's employees understand the importance and implications of IS and the extent to which they behave in accordance with organizational security policies and procedures is called IS awareness (ISA), and is an important element in protecting the organization from security breaches (Parsons et al., 2017).

Although there is a large amount of scientific research on the topic of IS, there are few instruments for ISA assessment that can be put to use. More specifically, organizations that conduct annual surveys on IS (e.g., Global State of Information Security Surveys - Pricewaterhouse) collect data on security breaches and their impact, but do not represent the experiences and opinions of employees (Parsons et al., 2014). Also, there are numerous methodological objections to such research, such as the choice and design of questions, the selected sample, statistical reporting, as well as the fact that they are often sponsored by organizations that sell security solutions (Anderson et al., 2012, Parsons et al., 2014). Some research aims to verify certain behavioral models (e.g., the Theory of Planned Behavior), which is why it includes only the variables covered by the theory and potentially omits other important variables (Bulgurcu et al., 2010; Pearson et al., 2017). Other research covers only narrow, specific IS areas, such as password use (Stanton et al., 2005) and smartphones (Clarke et al., 2016), or is generic and asks general questions about IS (Bulgurac et al., 2010; Haeussinger and Kranz, 2013). Such surveys are useful for gaining IS insights, but are unable to provide a comprehensive picture of ISA at the organizational level.

More recently, there have been several attempts to develop a holistic measure of ISA that would meet the practical needs of organizations. Some of them are: Users' Information Security Awareness Questionnaire (UISAQ; Velki et al., 2015), Security Behavior Intentions Scale (SeBIS; Egelman and Peer, 2015) and Human Aspects of Information Security Questionnaire (HAIS-Q; Parsons et al., 2017). The UISAQ covers potential security risk behaviors and the information system users' knowledge and awareness at the workplace, but also in their private life. SeBIS is focused on self-reported adherence to computer security advice in relation to device securement, password generation, proactive awareness and updating. HAIS-Q examines knowledge about the most common information system users' behaviors that lead to security breaches, as well as their attitudes and the frequency of such behaviors.

Our aim was to translate and validate HAIS-Q on the Croatian population. We wanted to have a questionnaire that would enable a quick, cost-efficient and comprehensive assessment of the level of ISA at work, as well as monitoring the effectiveness of targeted interventions. Regarding set conditions, the questionnaire that we found to be the most suitable for the starting point of developing a questionnaire applicable to the Croatian population is HAIS-Q (Parsons et al., 2017).

HAIS-Q

HAIS-Q was designed to assess ISA in Australian public sector employees, and was developed in several phases. Rather than focusing solely on theory verification, the authors used a hybrid methodology, incorporating the inductive, exploratory approach, and combining qualitative and quantitative methods for gathering and analyzing data (Parsons et al., 2013). In the first phase, interviews were conducted with senior management of each organization, and they highlighted human error, i.e., employee naivety, as the most problematic area of IS (Parsons et al., 2014). Accordingly, initial qualitative research was conducted, and several IS policies were reviewed. The findings were used to develop specific focus areas, designed to represent the areas of an IS policy that are most relevant to the employees and the employers, and which also cause the most common human errors (Parsons et al., 2014; Parsons et al., 2017).

The questionnaire is primarily focused on random, unintentional behaviors that are considered human errors. Their intention is not to harm the organization or its resources, but they are associated

with naivety and unawareness. For each of the seven areas, three sub-areas were defined that represented the most common human errors. Given that the questionnaire is based on the knowledge-attitude-behavior model (KAB model), for each of these sub-areas, one claim related to knowledge, attitude and behavior was developed. The KAB model is based on the assumption that increasing employees' knowledge of safe IS-related behaviors in the workplace improves their attitude, resulting in improved IS-related behaviors (Parsons et al., 2014).

Method

The aim of this research was to adapt and validate HAIS-Q on the Croatian population. In order to check criterion validity, in addition to HAIS-Q, the participants filled out UISAQ and several additional questions related to IS, which represent some of the possible aspects of computer users' risky behavior. The participants also filled out the socio-demographic data questionnaire.

Participants

In order to participate in the research, the participants had to meet the following conditions: they had to be employed, had to use a computer during working hours, and their organization had an IS policy/directive. The sample was heterogeneous with respect to the organization they work in, due to a security issue with completing the questionnaire in one organization.

The preliminary research was conducted on a sample of 18 participants (12 men and 6 women), with an average age of 32.5 years (*SD* = 2.35).

The main study was conducted on a sample of 337 participants with an average age of 40 (SD = 7.70). Most of the participants were between 31 to 40 (41.6%), and the fewest were aged 51 and above (6.3%). There were 12.3% of participants between 21 to 30, and 39.8% between 41 to 50 years of age. There were 24.3% of women and 75.7% of men in the sample. The participants were heterogeneous in terms of education: 29.4% completed secondary education, 26.1% completed a bachelor degree (post-secondary level), 38.9% have further graduate qualifications (university level), and 5.6% have completed a master's degree or doctorate (MSc. or MSc./Ph.D.).

Instruments

HAIS-Q (Parsons et al., 2017) consists of 63 items divided in seven focus areas of IS: *Password Management, Use of Email, Use of the Internet, Use of Social Networks, Use of Portable Devices/Telecommunication, Information Handling and Incident Reporting*. Each focus area is further divided into three sub-areas resulting in a total of 21 items. Each focus area consists of three items formulated so that the first refers to knowledge, the second to attitudes, and the third to behavior. For example, in the *Password Management* focus area and *Using the same password* sub-area, there are three items that examine:

- knowledge: "It is acceptable to use my passwords for social networks as the passwords of my user computers that I use for work."
- attitudes: "It is safe to use the same passwords on social networks and user accounts that I use for work."
- behavior: "I use different passwords on social networks and user accounts that I use for work.".

The scope of responses on each item ranges from 1 (strongly disagree) to 5 (strongly agree). A higher score in the questionnaire reflects a higher level of awareness. The reliability of the questionnaire (Cronbach Alpha) ranges from .75 to .82 (Parson et al., 2017).

UISAQ (Velki et al., 2015) consists of 33 questions grouped into two scales. The first is the *Computer Users' Risky Behavior Scale* (k=17), which consists of three subscales: *Computer Users' Common Risky Behaviors subscale* (k=6), *Personal Computer Systems Maintenance Subscale* (k=6) and *Borrowing Access Data Subscale* (k=5). The second is the *Information Security Knowledge Scale* (k=16), which

also consists of three subscales: *Degree of Computer Communications Security Subscale* (k=5), *Beliefs About the Computer Data Security Subscale* (k=5) and *Importance of Proper Computer Data Protection Subscale* k=5). Participants are asked to respond on a Likert-type scale, ranging from 1 to 5, where the answers offered have different meanings depending on the question asked (e.g., frequency, degree of security, degree of conviction, degree of personal data security importance). A higher score in the questionnaire reflects a higher level of awareness. The reliability of the questionnaire (Cronbach Alpha) ranges from 0.66 to 0.89. The questionnaire was used with the authors' permission.

The participants also answered several additional questions related to IS, which represent some of the possible aspects of computer users' risky behavior, as well as some socio-demographic questions. They were asked to estimate their workplace password strength, the number of people who know their workplace password, and to state if their organization has any legal document regulating IS.

Procedure

The research was conducted in several phases. In the first phase, HAIS-Q was translated and adapted for application to the Croatian population. This involved the collaboration of psychologists, translators and information security experts. It was translated from English to Croatian by a professional translator, and revised by an IS expert in order to check the comprehensibility of the items in the Croatian language due to specific expressions. More specifically, one of the more demanding tasks was the translation of professional terms for which there are still no agreed terms in the Croatian language, so the original English terms are often used instead (e.g., work accounts, password, print-out, hard-copy, USB...). Also, the items were cross-checked with several IS regulations from different organizations to ensure the accuracy and relevance of the items. Given that the questionnaire, among other things, examines knowledge of rules related to IS, we wanted to be sure that all the behaviors included in the questionnaire are listed in Croatian regulations, guidelines or instructions related to IS. Given that all items were covered by IS regulations, they were all retained. Afterwards, a reverse translation was carried out by another professional translator. Since no major differences between original and translated version were observed, the translation was considered adequate. Two IS experts fill it out using the cognitive interview technique - filling out the questionnaire while thinking aloud, and the interview afterwards, to check understanding of concepts, clarity of instructions and all other areas of potential misunderstanding. Most of the objections were related to the translation of professional terms which are not commonly used in Croatian (and are therefore sometimes confusing if translated), but mostly remain untranslated and are used in English. In the second phase, a pilot study was conducted on 18 participants. Following their feedback, some items have been simplified and certain terms changed. The term work account (Croatian: radni račun) was replaced with "poslovni korisnički račun", USB (Croatian: memorijski štapić) with "prijenosna memorija", email (Croatian: elektronička pošta) with "e-poruka", and for some terms such as password (Croatian: zaporka), print-out (Croatian: ispis), USB (Croatian: prijenosna memorija) and link (Croatian: veza), the English terms were left in brackets. In the third phase, we have applied the paper-pencil anonymous questionnaire to 337 respondents. Snowball sampling was used.

Results

Table 1 shows descriptive indicators and reliability for seven HAIS-Q scales (focus areas).

Sensitivity was calculated by the range of obtained results. Although the full range of responses is not obtained when we analyze total results on particular scales, the responses on individual items are distributed in the full range of possible responses. The distribution on all scales is negatively asymmetric, i.e., the results are shifted towards higher values as expected. The highly rated ISA was assessed for Use of Mobile Phones, Use of Social Networks and

Table 1. Descriptive indicators and reliability for seven HAIS-Q scales (focus areas) as well as knowledge, attitudes and behavior scales

	M	SD	Possible range	Min.	Max.	Skewness (SD)	Kurtosis (SD)	α
Password management	38.78	5.41	9-45	20	45	-0.74 (0.13)	-0.12 (0,27)	.68
Email use	35.82	6.59	9-45	17	45	-0.48 (0.13)	-0.43 (0,27)	.71
Internet use	37.32	6.48	9-45	13	45	-0.68 (0.13)	-0.28 (0,27)	.78
Social media use	39.98	5.45	9-45	22	45	-1.21 (0.13)	0.69 (0,27)	.66
Mobile devices	40.08	5.88	9-45	22	45	-1.20 (0.13)	0.46 (0,27)	.79
Information handling	39.98	5.45	9-45	22	45	-1.21 (0.13)	0.69 (0,27)	.75
Incident reporting	37.89	6.02	9-45	22	45	-0.57 (0.13)	-0.68 (0,27)	.80
Knowledge	86.81	12.26	21-105	47	105	-0.79 (0.13)	-0.03 (0,27)	.82
Attitudes	91.44	12.14	21-105	30	105	-1.37 (013)	2.28 (0,27)	.88
Behavior	88.08	10.99	21-105	42	105	-0.92 (0.14)	0.36 (0,27)	.83

Use of Information area, and the weakest for Use of the Internet and Use of E-mail area.

In order to check whether the respondents differ according to age, we divided them into 3 groups: younger age (≤35; N=109), middle age (36-50; N=204) and older age (≥51; N=21). The Kruskal-Wallis test of variance analysis was applied. Significant age differences were obtained on two scales: younger participants have significantly lower ISA when it comes to Password Management than middle-aged participants (H(2)=-33.31, p=.01), and lower ISA on the Incident Reporting scale than middle-aged (H(2)=-28.88, p=.04) and older-aged participants (H(2)=-61.45, p=.03). There are no statistically significant gender differences.

When it comes to the knowledge, attitudes and behavior scales, a statistically significant age difference was obtained only for behavior, whereby younger participants behave more risky than middle-aged ones (H(2)=-29.03, p = .03). There are no statistically significant gender differences.

In order to check the internal reliability, the Cronbach's Alpha coefficients were calculated (Table 1). They span from .66 to .80 for seven focus areas, and from .82 to .88 for knowledge, attitudes and behavior, which provides evidence of high re-

Table 2. HAIS-Q correlation matrix with criterion variables

	Password strength	Password sharing	UISAQ -CURB scale	UISAQ -ISK scale	UISAQ -total result
Password management	.28**	-.27**	.65**	.2**	.62**
Email use	.13*	-.11*	.46**	.26**	.46**
Internet use	.14*	.10	.48**	.30**	.48**
Social media use	.08**	-.11*	.54**	.31**	.54**
Mobile devices	.17**	-.07	.59**	.36**	.59**
Information handling	.08	-.11*	.54**	.31**	.54**
Incident reporting	.23**	-.17**	.60**	.30**	.60**
Knowledge	.18**	-.10	.53**	.37**	.56**
Attitudes	.13*	-.11*	.57**	.33**	.57**
Behavior	.25**	-.24**	.74**	.35**	.69**
HAIS-Q total	.21**	-.17**	.68**	.42**	.69**

Note. *p<.05, **p<.01

liability and indicates that the scales measure the same construct. Furthermore, correlation analyses were performed on seven focus area scales separately for knowledge, attitudes and behavior, and statistically significant positive correlations were obtained in the range from .23 to .69, which indicates a strong connection, but not multicollinearity. This provides justification for calculating the overall score on the knowledge, attitude and behavior scales.

In order to assess construct validity of HAIS-Q, specifically, convergent validity, a series of Pearson product moment correlation coefficients were conducted to examine the relationship between the HAIS-Q results and risk behavior assessments (password sharing and password strength), as well as between the HAIS-Q results and the UISAQ results (Table 2).

Participants who are more likely to share their passwords and generate weaker passwords have lower ISA on almost all HAIS-Q scales. All the correlations between the HAIS-Q and UISAQ results are statistically significant in the expected direction, and the total scores are strongly correlated (.69).

Discussion

The research results show that HAIS-Q is applicable for measuring ISA. On the one hand, the questionnaire enables an overview of the greatest IS risks within the framework of human aspects in the organization, while on the other hand, it provides information for designing interventions, measuring the effectiveness and impacts of training interventions, information security awareness programs and campaigns (McCormarc et al., 2017). Also, the collected data should foster improvements in existing security measures of the organization or development of the new ones.

For the purpose of questionnaire validation, data was collected in multiple organizations, considering that this type of data is highly sensitive and often classified since it reveals potential vulnerabilities of the organization. It was assumed that most organizations should have similar IS regulations. With this in mind, interpretation of the research results, when it comes to the knowledge scale, must be taken with caution. In order to obtain maximum benefit from the HAIS-Q results, it is important to align questionnaire items with the IS regulations in a particular organization, especially in the knowledge scale.

HAIS-Q showed good sensitivity. The results tend to group towards higher values, which indicates higher ISA. It can be assumed that most employees have some basic ISA when using computers and handling sensitive data in general. Full range of responses obtained for every item indicates that the questionnaire can distinguish even minor differences in the assessment of seven ISA focus areas.

Even though the differences in knowledge, attitudes and behavior for each of the seven focus areas showed good sensitivity and great practical use when we used it in our organization, this data is confidential and exceeds the scope of this paper.

The tendency of increasing ISA with age can be seen for all seven focus areas, but two scales showed statistically significant difference. Younger employees have a significantly lower ISA when it comes to Password Management than middle-aged participants, and a lower ISA in the Incident Reporting focus area than middle-aged and older participants. Perhaps they are less cautious and more willing to use different information systems. Also, they might have fewer negative direct and indirect experiences related to IS violations. Incidents related to security breaches occur rarely, so people are often convinced that such things cannot and will not happen to them. However, older employees may have encountered security breaches during their career or participated in IS educations, and accordingly developed greater awareness.

Furthermore, there is no statistically significant age difference in knowledge and attitudes, but there is when it comes to behavior. Middle-aged employees follow the rules more than younger employees. Regardless of equal knowledge and attitudes about IS rules, differences in behavior can perhaps be explained by a generally higher willingness to take risks among younger people, openness

to experiences and less experience with security breaches. According to Ma et al. (2010), in comparison to younger people (under 30 years of age), older employees showed less risky behavior. The peak of secure behavior is reached in middle adulthood, which is the most responsible period of life (people between 30 and 50 are usually married, have children, care about older family members, have carriers, etc., which makes them more responsible and aware of risks), and then it declines slightly again within the older age group (Velki & Romstein, 2018).

The research results showed satisfactory reliability of HAIS-Q. The correlation analyzes between HAIS-Q and criterion variables provide evidence for the construct validity of HAIS-Q. Individuals who generate stronger passwords show higher levels of ISA in all HAIS-Q focus areas except Information Handling. Also, they have higher results on knowledge, attitudes and behavior scale. Furthermore, sharing password with others is associated with a lower level of ISA in the areas of Password Management, E-mail use, Social Network Use, Information Handling and Incident Reporting, and generally lower scores on the attitude and behavior scale. An interesting fact is that this risky behavior is not related to the knowledge scale, which was unexpected, but some of the research participants provided a possible explanation. More precisely, a large number of employees, especially during the COVID-19 pandemic, were instructed to share their passwords with their colleagues, so that they could complete their tasks in the event of their absence. Accordingly, regardless of their knowledge of this rule, the employees followed the superiors' instructions. Correlations with UISAQ, which measures the same construct, are positive and statistically significant (high for the Computer Users' Risky Behavior Scale and moderate for the IS Knowledge Scale). The total score on UISAQ is also strongly positively correlated with all HAIS-Q scales, as well as with the total HAIS-Q score (.69), which is all in favor of high external validity, and indicates that the same construct is being measured.

Conclusion

HAIS-Q can be used for a simple and quick ISA assessment and as a basis for improving IS. The information obtained through the use of the questionnaire indicates the weakest links of IS, and enables targeted guidance for education. In subsequent research, it is important to use a homogeneous sample of examinees with regard to the IS policy of the organization. Also, further research is needed to determine the key factors influencing ISA (age, level and field of education, personality traits etc.)

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M., Levi, M., Moore, T., & Savage, S. (2012). Measuring the cost of cybercrime. *Proceedings of the 11th workshop on the economics of information security (WEIS)* (pp. 265-300). https://doi.org/10.1007/978-3-642-39498-0_12.

Arbanas, K. (2020). Ključni čimbenici kulture informacijske sigurnosti (Key factors of information security culture). *Policija i sigurnost*, 29, 376-388. https://hrcak.srce.hr/247822

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34, 523-548. https://doi.org/10.2307/25750690

Clarke, N., Symes, J., Saevanee, H., & Furnell, S. (2016). Awareness of mobile device security. *International Journal of Mobile Computing and Multimedia Communications*, 7(1), 15–31. https://doi.org/10.4018/IJMCMC.2016010102

Egelman, S., & Péer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (pp. 2873-2882). New York, NY: ACM. https://doi.org/10.1145/2702123.2702249

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of

security. *Computers & Security*, 31. 983–988. https://doi.org/10.1016/j.cose.2012.08.004

Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior. *Proceedings of the 34th international conference on information systems (ICIS), Milan, Italy.* https://www.researchgate.net/publication/258926834_Information_Security_Awareness_Its_Antecedents_and_Mediating_Effects_on_Security_Compliant_Behavior

Ma, W., Campbell, J., Tran, D., & Kleeman, D. (2010). Password entropy and password quality. *Proceedings of the 4th international conference on network and system security, NSS* (pp. 583-587). https://doi.org/10.1109/NSS.2010.18.

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. *Proceedings of the 5th international conference on research and innovation in information systems (ICRIIS)* (pp. 1-6). Langkawi, Malaysia: IEE. https://doi.org/10.1109/ICRIIS.2017.8002442

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems, 21.* https://doi.org/10.3127/ajis.v21i0.1697

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66(2), 40-51. https://doi.org/10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security,* 42, 1-12. https://doi.org/10.1016/j.cose.2013.12.003

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2013). The development of the human aspects of information security questionnaire (HAIS-Q). In H. Deng, & C. Standing (Eds.), *ACIS 2013: Information systems: transforming the future: Proceedings of the 24th Australasian conference on information systems*, Melbourne, Australia, (pp. 1-11). https://www.researchgate.net/publication/286610727_The_development_of_the_human_aspects_of_information_security_questionnaire_HAIS-Q

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013a). An analysis of information security vulnerabilities at three Australian government organisations. *Proceedings of the European information security multi-conference, EISMC* (pp. 34-44). https://www.researchgate.net/publication/ 286612263_An_analysis_of_information_security_vulnerabilities_at_three_Australian_government_organisations

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

Velki, T., & Romstein, K. (2018). User risky behavior and security awareness through lifespan. *International journal of electrical and computer engineering systems*, 9(2), 53-60. https://doi.org/10.32985/ijeces.9.2.2

Velki, T., Šolić, K., & Nenadić, K. (2015). Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava [Development and validation of the information system user knowledge and risk behavior questionnaire]. *Psihologijske teme*, 24 (3), 401-424. https://urn.nsk.hr/urn:nbn:hr:141:984004

Yoo, H., Lee, J. H., & Chung, J. (2019). An analysis of the survey results on nuclear security culture for personnel at nuclear facilities. *Progress in Nuclear Energy*, 112(1), 75-79. https://doi.org/10.1016/j.pnucene.2018.12.007