Advances in Informatics, Management and Technology in Healthcare
J. Mantas et al. (Eds.)

doi:10.3233/SHTI220650

Assessing Internal Consistency of HAIS-Q: A Survey Conducted in Greek Hospitals

Andriana MAGDALINOU[a,1], Athena KALOKAIRINOU[a], Flora MALAMATENIOU[a] and John MANTAS[a]
[a]*National and Kapodistrian University of Athens, Greece*

Abstract. Despite the prevailing perception that powerful software and hardware are adequate solutions to minimize information systems' security breaches, privacy remains at stake. Human factors play an important role in maintaining information security as it is evident that non secure practices applied by employees may increase the vulnerability of the systems and lead to privacy issues. Non secure practices found in literature are related to the use of Internet, the use of emails, password management, information handling and incidence reporting. For this purpose a survey was designed to be conducted in seven hospitals in Greece in order to record non secure practices applied by nursing staff and identify correlation factors. This paper presents the reliability test of the HAIS-Q tool which was applied in order to conduct the survey entitled: Examining the Nurses' non secure IT practices in Greek Hospitals as well as the preliminary results of the study.

Keywords. Information Security, Non Secure Practices, Nursing

1. Introduction

As information technology evolves, data privacy gets compromised. The development of software per se cannot prevent security breaches and reduce threats. Human Factors play an important role as non secure practices followed by employees may increase systems vulnerability. According to relevant surveys, non compliance to policies related to information security, non secure practices followed by employees and inappropriate IT security measures can lead to multiple healthcare data breaches and cause financial losses and stigma to patients [1], [2].

More precisely, the most common non secure IT practices are accessing email and downloading inappropriate attachments [3], [4], using USB to transfer files [5], exchanging passwords [6], using the same password for long time periods, accounts remaining active after employee leaving the workspace [7], non reporting of security breach incidents [8], and allowing third parties to access the computer [9]. Knowledge of and staff attitude towards policies related to IT security, the self reporting perception of danger, training opportunities, the enforcement of IT security policies and the culture in the organization can affect employees IT security practices [10].

[1] Corresponding Author, Andriana Magdalinou, Nursing Department, National and Kapodistrian Univeristy of Athens, Papadiamantopoulou 123, Athens, Greece; E-mail: alfami@nurs.uoa.

This paper aims at presenting the reliability test of the HAIS-Q tool which was applied in order to conduct the survey entitled**:** Examining the Nurses' non secure IT practices in Greek Hospitals and publishing the first results of the study.

2. Methods

HAIS-Q tool [11] consisted of 63 items in a five-point Likert scale rated form Strongly Agree to Strongly Disagree was used. Researchers [11] were informed and consented to the use of the tool. The final version of the tool was translated into Greek by three researchers and included 45 Items related to Information management, Password Management, Email usage, Internet usage, and Incidence reporting. Items related to Social Networking Site use and Mobile Computing were removed as irrelevant to the healthcare sector in Greece. Hypotheses were formed: H1: Better attitude towards IT security policies and procedures is linked to less non secure practices, H2: Better knowledge of IT security policies and procedures is linked to less non secure practices. The final sample used to assess internal consistency of the tool was 165 registered nurses. SPSS software was used to analyze the data.

3. Results

HAIS-Q was administered to 165 nurses in order to assess internal consistency of the tool. The Cronbach's alpha for the construct of Knowledge of information security policies in the organization received a value of 0.701 while for the construct of Attitude of the employees in information security policies received a value of 0.749. The Cronbach's alpha for the construct of the Information Security Practices of the employees in their workplace was estimated 0.725. Finally, the Cronbach's alpha for Employee Awareness of Information Security received a value of 0.89.

Table 1. Reliability test for HAIS-Q.

Constructs	Cronbach's alpha
Knowledge of policies	0.701
Attitudes towards policies	0.749
Information Security Practices	0.725
Awareness of Information Security	0.89

The demographics of the sample show that 82.4% of the participants were women while 17.6% were men. 38.2% of the participants were in the age group 40-50, 27.9% were between 29-39, 20.6% aged 51-61, 9.1% aged 18-28 and 4.2% were over 61 years old. 33.9% of participants have worked for more than 15 years in the same organization, 22.4% from 11-15 years, 19.4% from 6-10 years, 13.9% from 1-5 years, while 9.7% were employed less than 1 year. Participants were informed about the information security policies in their organization either formally (51.5%) or informally (48.5%). Finally, 47.9% have not been informed by another source about information security while 52.1% have used other sources to learn about information security.

Preliminary results of the study regarding Nurses' knowledge of information security policies show that Nurses have average to sufficient knowledge regarding the password management and the reporting of breaches. Nurses report that they are not allowed to share passwords with colleagues and that they should not ignore the bad

security practices of their colleagues. They also state that if they see someone acting suspiciously in their workplace they would report it. Nurses' knowledge regarding the email management and the handling of information is average, and average to insufficient is their knowledge regarding the internet usage. Nurses report that they can visit any website while working. Nurses respond neutrally to questions about their attitude towards information security policies in the areas under study. However, they state that it is a bad idea to share their work passwords with others, even if requested by a colleague, and that it may be dangerous to download files to their work computer. They feel it is safe to use the same password for their social media accounts and work computer and consider that rejecting prints containing sensitive information by placing them in the trash is not safe. Nurses respond neutrally to their practices regarding email management, internet use, password management, information management, and reporting breaches. However, they report that they do not share their work passwords with colleagues and that they would not connect a USB they found in a public place to their workstations. Finally, regarding the correlations of the IT security practices applied by the nursing staff with the knowledge of and the attitude towards the IT security policies, it was deducted that there is a strong correlation of the variables.

4. Discussion

The HAIS-Q tool was translated into Greek and the final version included five focus areas with 45 items in total. In our study, the internal consistency was assessed using a sample of 165 nurses. Cronbach's alpha for the Knowledge of information security policies was 0.701, for the Attitude of the employees towards information security policies was 0.749 and for the Information Security Practices was 0.725. Cronbach's alpha was estimated 0.89 for the Total Awareness of Nurses regarding Information Security which is considered sufficient. Therefore the tool used was considered reliable. In comparison to our results, a validation study was performed by the researches who developed the tool [11] using Cronbach's alpha coefficient which was estimated above 0.87 for Knowledge, and Attitude and equal to 0.9 for Self Reported Practices. In another validation study [12] internal consistency exceeded the Cronbach's alpha coefficient of 0.70 and for each focus areas scored between 0.75 and 0.82. A study [13] followed where HAIS-Q was administered to a sample of 51 people assessing the internal consistency with Cronbach's alpha exceeding 0.7. In our study, the Nurses' overall Information Security Awareness range from average to sufficient and up to our knowledge this is the first attempt to estimate Nurses' Knowledge, Attitude and Practices regarding information security in the healthcare sector. In a study [14] where HAIS-Q was implemented in 25 companies in Indonesia the results showed an average level of Information Security Awareness. As found in our study there is positive correlation between Information Security Practices applied by the Nursing staff and the Knowledge of the Information Security policy as well as positive correlation between Information Security Practices and the Attitude towards the Information Security Policies. This is similar to the findings [11] that better Knowledge and Attitude towards Policy and Procedures are both associated with Information Security Practices that are more prudent.

5. Conclusions

The tool used was considered reliable and can be distributed to the study population. The preliminary results of the study showed the level of Knowledge of and Attitude of the Nurses towards the Information Security Policy in their organization and the correlation of the variables were also estimated. The overall Awareness of Nurses on issues related to Information Security of the organization in which they work range from average to sufficient, while specific areas such as Knowledge of Policies related to the use of the Internet could be improved through the commitment of the management in Information Security, the cultivation and promotion of an organizational culture that favors good Security Practices and the delivery of proper training and organization of relevant awareness programs. Future steps will include the analysis and dissemination of the final results of the research including the final sample of nurses who work in seven public hospitals in Greece.

References

[1] Gaunt N. Practical approaches to creating a security culture. International Journal of Medical Informatics. 2000;60(2):151-157.
[2] Albrechtsen E. A qualitative study of users' view on information security. Computers & Security. 2007; 26(4):276-289.
[3] Silvius AJ, Dols T. Factors influencing Non-Compliance behavior towards Information Security Policies. In: CONF-IRM Proceedings; 2012.p.39.
[4] Alqahtani FH. Developing an Information Security Policy: A Case Study Approach. Procedia Computer Science.2017;124:691-697.
[5] Guo KH, Yuan Y. The effect of multilevel sanctions on information security violations: A mediating model. Information & Management.2012;49(6):320-326.
[6] Hedström K, Karlsson F, Kolkowsk E. Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. Information Management & Computer Security.2013;21(4):266-287.
[7] Connoly L, Lang M, Tygar J. Investigation of Employee Security Behaviour: A Grounded Theory Approach. In: 30th IFIP International Information Security Conference (SEC); May 2015; Ham burg, Germany;2015.p.283-296.
[8] Kirlappos I. Learning from Shadow Security: Understanding Non-Compliant Behaviours to Improve Information Security Management. University College London;2016.
[9] Hovav A, D'Arcy J. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. Information & Management.2012;49(2):99-110.
[10] Topa I, Karyda M. Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance. In: Fischer-Hübner, S, Lambrinoudakis C, López J, editors. Trust, Privacy and Security in Digital Business; Lecture Notes in Computer Science; Springer, Cham;2015.p.169-179.
[11] Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & Security.2014;42:165-176.
[12] Parsons K, Calic D, Pattinson M, Butavicius M, McCormac A., Zwaans T. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security.2017;66:40-51.
[13] Zulfia A, Adawiyah R, Hidayanto N, Fitriah N. Measurement of Employee Information Security Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case Study at PT. PQS.In: 5th International Conference on Computing Engineering and Design (ICCED). Institute of Electrical and Electronics Engineers Inc;2019.p.1-5.
[14] Mahardika MS, Hidayanto AN, Paramartha PA, Ompusunggu LD, Mahdalina R, Affan F. Measurement of Employee Awareness Levels for Information Security at the Center of Analysis and Information Services Judicial Commission Republic of Indonesia. Advances in Science,Technology and Engineering Systems Journal.2020;5(3):501-509.