https://dergipark.org.tr/tr/pub/ijhmt Doi Number: 10.31201/ijhmt.791913

Int Journal Of Health Manag. And Tourism 2020, 5(3), 336-347

JHMT Editorial

Internatıonal Journal Of Health Management And Tourism

# THE EFFECTS OF INFORMATION SECURITY TRAINING ON EMPLOYEES: A STUDY FROM A PRIVATE HOSPITAL

Gökhan ÖZASLAN[1], Pınar KILIÇ AKSU[2] ,Büşra TEKİN[3], Nur ŞİŞMAN KİTAPÇI[4], Okan Cem KİTAPÇI[5], Leyla KÖKSAL[6], Gonca MUMCU[7]

[1] Health Manager in a Private Hospital, Turkey, ozaslangokan@hotmail.com,
ORCID Number: 0000-0003-2237-4233

[2] Asst. Prof. Department of Health Management, Yeditepe University, Turkey, pinarkilicaksu@yahoo.com,
ORCID Number: 0000-0002-8040-2151

[3] R.A. Department of Health Management, Sağlık Bilimleri University, Turkey, busra.tekin@sbu.edu.tr,
ORCID Number: 0000-0002-6143-6954

[4] Asst. Prof. Department of Health Management, Marmara University, Turkey, nsisman@marmara.edu.tr,
ORCID Number: 0000-0002-4766-5662

[5] Dr. Department of Health Management, Marmara University, Turkey, okancem.kitapci@marmara.edu.tr,
ORCID Number: 0000-0001-7584-3297

[6] Asst. Prof. Department of Health Management (Emeritus), Marmara University, Turkey, leylakoksal@gmail.com,
ORCID Number: 0000-0001-6993-1645

[7] Prof. Dr. Department of Health Management, Marmara University, Turkey, gonca.mumcu@gmail.com,
ORCID Number: 0000-0002-2280-2931

Received: 08.09.2020
Accepted: 31.10.2020
Research Article

## Abstract:

Aim: Human error is known as the biggest threat to information security in healthcare organizations. Training on the information security is important to the mission of establishing sustainable information security. The aim of the study was to evaluate the effect of a training program for information security in a private hospital.

Materials and Methods: In this cross-sectional study, 66 medical unit employees (M/F: 53/13, mean age: 30,27±11,12 years) and 34 administrative unit employees (M/F: 11/23, mean age: 31,5±10,84 years) using

the Hospital Information Management System (HIMS) were included. Data were collected by a questionnaire regarding the validated Information Security Scale before and after the training program.

Results: Scores of Security Policy, Security Applications, Access and Authorization subgroups were significantly improved by the training program in both medical and administrative staff ($p<0.05$). However, these scores in pre-test and post-test were found to be similar in both groups ($p>0.05$). In addition, there was no positive effect of HIMS training on scores of these subgroups ($p>0.05$).

Conclusion: Well-designed training programs are necessary for improving information security culture in hospitals. Since ensuring the appropriate protection of organizational assets, it is essential to design an effective training program regarding information security and privacy in the perspective of health managers.

**Keywords:** *Information security, Privacy, Information security training, Private hospital*

## Introduction

Information and communication technologies (ICTs) are increasingly used in healthcare. The use of ICTs in healthcare services contributes positively to service delivery by increasing service quality and patient safety, ensuring the efficiency of financial and administrative activities, storing data easily and having access to the system for many users (Delgado et.al, 2016). Although they offer numerous benefits, risks of security and privacy are copying or sharing of username/password and patient information or visible patient information on device screens. Data security breaches are growing concerns (Arain et.al, 2019).

Information security and technology use are two essential components in the provision of healthcare services (Mumcu et.al, 2014; Wilkowska et.al, 2012). Moreover, users have important roles to contribute institutions' information security performance as well as security awareness and cautious behavior (Schattner et.al, 2007; Stanton et.al, 2005). Accessibility, integrity and confidentiality of electronic medical records are important issues for providing healthcare services (Kruse et.al, 2017). It should also be kept in mind that negative situations such as attacks on medical records, changing records or blocking access to records are significant risks for all stakeholders involved in service delivery (Desjardin et.al, 2020).

Since the healthcare environment involves several stakeholders, namely the patient, the healthcare provider, researchers, and third-party payers, unauthorized access or any failure of the information security are critical points for the perspective of health management. Security breaches are threats that they also result in both direct and indirect costs. The data security is ensured by the application of technical controls, well-designed operational plans, policies and awareness and training (Box

and Pottas, 2013; Ahlan et.al, 2015). Since it is important for organizations to create a security-conscious culture, each organization has its own information security culture. Culture has influenced by the formation of many security measures, such as national security policy, information ethics, security training, and privacy issues (Gebrasilase and Ferede, 2011). Organizations should make continual efforts to ensure that the content of policy is effectively communicated to the employees (Ghazvini and Shukur, 2016). Therefore, the factors that play a significant role in shaping perceived security should be enhanced (Peikari et.al, 2018).

Training programs for information security are required by all organizations because they need to protect their valuable assets. The employees play an enormous role in information security. As many organizations are envisaging new threats and challenges in information security, the training programs should be flexible and adjustable to meet the current and future challenges. A sustainable training program would have been established to meet the future need. The training program will also accord the users to realize the knowledge of sensitive and personal data, knowledge of the organization security goals, security policies and the skills needed towards information security management (Olusegun and Ithnin, 2013).

Since training programs are effective approaches to reduce the risks in electronic health systems (Olusegun and Ithnin, 2013), the organizations can develop several training modules that target employees who need to be aware of their requirements for compliance based on legislative policies and acts (Arain et.al, 2019; Tsohou et.al, 2008). Employees have different levels of computer skills, thus they require to be trained differently. It is also observed that most of the trained employees do not attempt to apply the learned skills in the work environment. Moreover, many training programs do not measure users' performance before and after the training, and therefore, it is not possible to evaluate the training's outcome. Additionally, several employees are not motivated to contribute on the awareness-training program (Ghazvini and Shukur, 2016). Finally, human error is considered as the biggest threat to information security effectiveness owing to lack of employees' attention (Ghazvini and Shukur, 2016). Therefore, many organizations establish the awareness programs to ensure that their employees are informed about security risks, thereby protecting themselves and their profitability (Gebrasilase and Ferede, 2011).

Security policy is about making users aware of the value and importance of information and security procedures. Therefore, these programs are important approaches towards training users to prevent security incidents (Tsohou et.al, 2008).

The aim of this study was to evaluate the effect of an information security-training program for Hospital Information Management System (HIMS) in a private hospital.

## Materials and Methods

The study was carried out in a private hospital that had a total of 403 employees. The number of HIMS users was 313 in the hospital. Among them, 100 users participated in the study. Pre-tests were applied before information security training. Then, the training was performed. A week later, post-tests were carried out.

The data were collected by a structured questionnaire regarding the Information Security Scale validated by Kılıç Aksu et.al (2015). In addition, employees were asked whether training for HIMS was received or not. The health manager in the hospital chose three sub-group scores of the scale regarding "Security Policy", "Access and Authorization" and "Security Applications". The questionnaire was scored with a five-point Likert Scale (1: strongly disagree, 2: disagree, 3: neutral, 4: agree, 5: strongly agree). Low scores indicated good information security status. The study was performed according to the principles of the Declaration of Helsinki and was approved by the Ethical Committee of Marmara University Health Institute (15.04.2019-108).

**Statistical analysis**. Data were analyzed by using SPSS 26.0 statistic program (IBM, USA). The differences between Pre-test scores and Post-test scores were compared by Paired T test. Scores of different groups were analyzed by Unpaired T test. In the study, p value less than 0.05 was accepted as statistically significant.

## Results

**Table 1. The Profile of the Study Group**

| | | Medical Unit Employees | | Administrative Unit Employees | | Total | |
|---|---|---|---|---|---|---|---|
| | | n | % | n | % | n | % |
| Gender | Female | 13 | 19,70 | 11 | 32,30 | 24 | 24,00 |
| | Male | 53 | 80,30 | 23 | 67,70 | 76 | 76,00 |
| Age | 20-30 | 43 | 65,20 | 21 | 61,80 | 64 | 64,00 |
| | 31-40 | 11 | 16,70 | 10 | 29,40 | 21 | 21,00 |
| | 41-50 | 5 | 7,60 | 1 | 2,90 | 6 | 6,00 |
| | >50 | 7 | 10,60 | 2 | 5,90 | 9 | 9,00 |
| Graduation | High School | 25 | 37,88 | 16 | 47,05 | 41 | 41,00 |
| | University | 41 | 62,12 | 18 | 52,95 | 59 | 59,00 |
| Working period in the hospital | 0-1 years | 39 | 59,10 | 12 | 35,30 | 51 | 51,00 |
| | 1-2 years | 20 | 30,30 | 17 | 50,00 | 37 | 37,00 |
| | > 2 years | 7 | 10,60 | 5 | 14,70 | 12 | 12,00 |

In the study, the profile of the study group was seen in Table 1. When the working experience in the hospital was evaluated, 88% of employees were working in this hospital for less than 2 years (Table 1). When subgroup scores of the scale were examined in medical employees and

administrative employees, pre-test scores of them were found to be similar in the study (p>0.05) (Table 2 and Table 3).

**Table 2. Comparison of Pre-Test and Post-Test Scores of Information Security Scale of Medical Unit Employees**

| | | n | Mean | SD | p |
|---|---|---|---|---|---|
| **Security Policy** | Pre-test | 66 | 20,34 | 7,52 | **0.000** |
| | Post-test | | 14,56 | 3,19 | |
| **Access and Authorization** | Pre-test | 66 | 13,39 | 4,59 | **0.000** |
| | Post-test | | 10,71 | 1,87 | |
| **Security Applications** | Pre-test | 66 | 8,9 | 3,15 | **0.000** |
| | Post-test | | 6,22 | 1,58 | |

**Table 3. Comparison of Pre-Test and Post-Test Scores of Information Security Scale of Administrative Unit Employees**

| | | n | Mean | SD | p |
|---|---|---|---|---|---|
| **Security Policy** | Pre-test | 34 | 20,05 | 7,02 | **0.000** |
| | Post-test | | 14,88 | 2,69 | |
| **Access and Authorization** | Pre-test | 34 | 12,29 | 3,88 | 0.07 |
| | Post-test | | 10,94 | 1,89 | |
| **Security Applications** | Pre-test | 34 | 8,35 | 3,23 | **0.001** |
| | Post-test | | 6,11 | 1,64 | |

In medical employees, all subgroup scores were significantly decreased by the training compared to pre-test scores ($p<0.05$) (Table 2). When the pre-test and post-test scores of the employees working in the administrative unit were compared; decrease in scores were found in the sub-groups of "Security Policy" and "Security Applications" after information security training ($p=0.000$, $p=0.001$ respectively). Yet, no significant difference was found in the "Access and Authorization" subgroups ($p=0.07$) (Table 3).

The effectiveness of HIMS training on information security was also evaluated in the study. There were no significant differences observed in subgroups scores of employees whether HIMS training was received or not ($p>0.05$) (Table 4).

**Table 4. Pre-Test and Post-Test Scores of Information Security Scale in Employees According to Education Status for HIMS**

| | | | n | Mean | SD | p |
|---|---|---|---|---|---|---|
| **Pre-test** | **Security Policy** | Education (+) | 67 | 19,46 | 7,41 | 0.068 |
| | | Education (-) | 33 | 22,30 | 6,87 | |
| | **Access and Authorization** | Education (+) | 67 | 12,67 | 4,61 | 0.259 |
| | | Education (-) | 33 | 13,72 | 3,81 | |
| | **Security Applications** | Education (+) | 67 | 8,55 | 3,24 | 0.458 |
| | | Education (-) | 33 | 9,06 | 3,04 | |
| **Post-test** | **Security Policy** | Education (+) | 67 | 14,32 | 2,95 | 0.108 |
| | | Education (-) | 33 | 15,36 | 3,09 | |
| | **Access and Authorization** | Education (+) | 67 | 10,73 | 1,96 | 0.643 |
| | | Education (-) | 33 | 10,90 | 1,70 | |
| | **Security Applications** | Education (+) | 67 | 6,17 | 1,63 | 0.923 |
| | | Education (-) | 33 | 6,21 | 1,55 | |

## Discussion

Information security and privacy are important for medical unit employees in terms of protecting patient information, while administrative unit employees have responsibilities for the protection of institutional information (Sevimli et.al, 2019). The importance of information security training is emphasized in order to prevent user-related problems (Kılıç Aksu et.al, 2015). Employees of an organization are still the most variable, unpredictable and the most uncontrollable factor in the information security. They may consider themselves secure by using passwords for accessing computers or any data. But in fact, it does not hold truth because some of them might choose predictable passwords or might share it. All these could happen because employees are not aware of the importance of information security, or they may not have a clear understanding of the risk. Information security is a critical and complex task, it is not just using usernames and passwords as security measures (Tschakert and Ngamsuriyaroj, 2019; Hepp et.al, 2018). The most important factor in effective information security is to make all employees aware of their responsibilities and their roles in information security. Security awareness teaches them how to protect the organization's valuable information and how to take responsibility for preventing security breaches. The aim of information security awareness is to make positive changes in the behavior of the employees (Tschakert and Ngamsuriyaroj, 2019). Therefore, the aim of the study was to evaluate the effect of a training program for information security in a private hospital.

In the study, scores of "Security Policy", "Access and Authorization" and "Security Applications" subgroups in the Information Security Scale were decreased by the training in the medical unit employees. However, similar trend was seen in administrative unit employees, except "Access and Authorization" subgroup. Since Access and Authorization of the scale is critical component for administrative unit employees, these results were predicted.

Information security training should be an integral part of healthcare employees' continuing education to prevent potential breaches and protect patient information. The evaluation of the training program ensures that employees are aware of available resources and understand how to prevent ICTs security breaches. Employees' lack of awareness related to organizational ICTs policy and compliance requirements could potentially create more risk for security breaches (Arain et.al, 2019). Therefore, information security training is an important instrument to improve and

influence the knowledge, attitude, and behavior, for information security in the employees. Human error can be minimized through the training programs. The significance of information security is the best defined as the level of user comprehension of information security awareness. In every organization, employees have varying knowledge of information security awareness. These kinds of errors can be corrected through training programs with an intention to promote behaviors of individuals toward organizational policy. Training programs in organizations can help to improve employees' awareness toward the security of E-health systems and help them to adhere to appropriate behaviors that do not compromise the security of the system (Ghazvini and Shukur, 2016). Based on these facts, the information security awareness programs have positive influences on the employees' knowledge, attitude, and behavior in real life. It is strongly recommended to have management support, in order to promote the employees into massive participation (Tschakert and Ngamsuriyaroj, 2019; Hepp et.al, 2018). Therefore, employees' training is the greatest non-technical tool to protect information security in organizations (Fernández-Alemán et.al, 2015). Good training and efficient policies to deal with security threats are good sources of preventing security breaches in health organizations (Fernández-Alemán et.al, 2015; Veiga and Martins, 2015). Training can increase staff knowledge and awareness about the threats and consequences of a security breach, leading to the prevention of such incidents. Likewise, employees' training and monitoring can influence the security culture in organizations. Employee monitoring is used by organizations to ensure that their employees adhere to their rules and regulations. Accordingly, employee monitoring reduces the likelihood of an employee-related security breach by increasing their perception of certainty and severity of punishments and the potential consequences for such behaviors (Peikari et.al, 2018).

In the study, no significant difference was found in the pre-test and post-test subgroup scores of those who received HIMS training and those who did not. The use of HIMS has ensured the achievement of many purposes such as creating a cost advantage, saving time by efficiently using time, producing quality service, and protecting and improving health. In particular, it has enabled the service provision to the patient at the right time (Mumcu et.al, 2014). In this respect, HIMS training is of great importance. However, according to the results of the study, it is thought that HIMS training is not sufficient in terms of providing information security and privacy. This results could be predicted since the outlines of information security training are different from HIMS

training. It is thought that ensuring information security is possible by creating an institutional culture on this subject, increasing the awareness of the employees through information security and privacy training at regular intervals. According to the results, training is of great importance in ensuring information security and privacy.

This study showed the importance of information security training as well as lack of performance of HIMS training on information security. The main limitation of the study was that data were collected from a single hospital.

## Conclusion

Employees must be trained on how to handle information carefully according to the guidelines and to become aware of the possible consequences of their actions. Security training and awareness programs are even more critical to any comprehensive information security policy. It is essential to increase the effectiveness of information security training programs by encouraging employees to make an effort in transferring the learned skills to their daily job activities. Employees who interact with HIMS must be educated about the risks and hazards associated with information security. As a result, the security policy should be aligned with the readiness of the user's state of perception and emotion, as well as the user's environment.

## References

Ahlan, AR., Lubis, M. and Lubis, AR. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures, Procedia Computer Science, 72:361 – 373.

Arain, MA., Tarraf, R. and Ahmad, A. (2019). Assessing, Staff Awareness and Effectiveness of Educational Training on IT Security and Privacy in a Large Healthcare Organization, Journal of Multidisciplinary Healthcare, 12:73–81.

Box, D. and Pottas, D. (2013). Improving Information Security Behaviour in the Healthcare Context, Procedia Technology, 9:1093 – 1103.

Delgado, J., Llorente, S., Pàmies, M. and Vilalta, J. (2016). Security and Privacy in a DACS, Exploring Complexity in Health: An Interdisciplinary Systems Approach, European Federation for Medical Informatics (EFMI) and IOS Press, 122-127.

Desjardin, B., Mirsky, Y., Ortiz, MP., Glozman, Z., Tarbox, L., Horn, R. and Horii, SC. (2020). Dicom Images Have Been Hacked! Now What? American Journal of Roentgenology, 214(4):727-735.

Fernández-Alemán, JL., Sánchez-Henarejos, A., Toval, A,. Sánchez-García, AB., Hernández-Hernández, I. and Fernandez-Luque, L. (2015). Analysis of Health Professional Security Behaviors in a Real Clinical Setting: An Empirical Study, Internatioal Journal of Medical Informatics, 84(6):454–67.

Gebrasilase, T. and Ferede, LL. (2011). Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital, The African Journal of Information Systems, 3(3): Article 1.

Ghazvini, A., Shukur, Z. (2016). Awareness Training Transfer and Information Security Content Development for Healthcare Industry, International Journal of Advanced Computer Science and Applications, 7(5):361-370.

Hepp, SL., Tarraf, RC., Birney, A. and Arain, MA. (2018). Evaluation of the Awareness and Effectiveness of IT Security Programs in a Large Publicly Funded Health Care System, Journal of the Health Information Management Association of Australia, 47(3):116-124.

Kılıç Aksu, P., Şişman Kitapçı, N., Çatar, RÖ., Köksal, L. and Mumcu, G. (2015). An Evaluation of Information Security from the Users' Perspective in Turkey, Journal of Health Informatics in Devoloping Countries, 9(2):55-67.

Kruse, CS., Smith, B., Vanderlinden, H. and Nealand, A. (2017). Security Techniques for the Electronic Health Records, Journal of Medical Systems, 41(8):127.

Mumcu, G., Köksal, L., Şişman, N., Çatar, RÖ. and Tarım, M. (2014). The Effect of Pharmacy Information Management System on Safety Medication Use: A Study from Private Hospitals in İstanbul. Marmara Pharmaceutical Journal, 18:1-4.

Olusegun, OJ. and Ithnin, NB. (2013). People are the Answer to Security: Establishing a Sustainable Information Security Awareness Training (ISAT) Program in Organization, International Journal of Computer Science and Information Security, 11(8): 57-64.

Peikari, HR., Ramayah, T., Shah, MH. and Lo, MC. (2018). Patients' Perception of the Information Security Management in Health Centers: The Role of Organizational and Human Factors, BMC Medical Informatics and Decision Making, 18:102.

Schattner, P., Pleteshner, C., Bhend,H. and Brouns, J. (2007). Guidelines for Computer Security Ingeneral Practice, Informatics in Primary Care, 15:73-82.

Sevimli, E., Altingöz, EN., Şisman Kitapçı, N., Kitapçı, OC., Köksal, L., Yay, M., Kılıç Aksu, P. and Mumcu, G. (2019). An Assessment of Health Information Systems Through the Perspective

of Computer Engineering Students and Medical Students, Acta Informatica Medica, 27(5):300-304.

Stanton, JM., Stam, KR. and Mastrangelo, P. (2005). Analysis of End User Security Behaviors, Computers & Security, 24(2):124-133.

Tschakert, KA. and Ngamsuriyaroj, S. (2019). Effectiveness of and User Preferences for Security Awareness Training Methodologies, Heliyon, 5(6).

Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps, Information Security Journal A Global Perspective. 17(5-6):207-227.

Veiga, AD. and Martins, N. (2015). Improving the Information Security Culture Through Monitoring and Implementation Actions Illustrated Through a Case Study, Computers&Security, 49: 162–76.

Wilkowska, W. and Martina, Z. (2012). Privacy and Data Security in E-health: Requirements from the User's Perspective, Health Informatics Journal, 18(3):191–201.