INFLUENCE OF USER'S PERCEPTION ON SECURITY OF ELECTRONIC HEALTH RECORDS IN TANZANIA PUBLIC HOSPITALS

Authors

Ernest Godson and Dr. Thadei Kiwango

Department of Informatics

Institute of Accountancy Arusha

&

Department of Informatics

Institute of Accountancy Arusha

Abstract:

Human factor is an important component in the security of information in organizations, as human factor determine the behavior of the users of information toward information security controls in organization. This paper attempt to assess the influence of user's perception of security on security of electronic health records. The study adopted a descriptive research design. Data were collected at Mount Meru Regional Referral hospital in Arusha. Quantitative research approach were used. A purposive non-probability sampling technique was applied to select a total number of 75 participants, out of 75 participants who were contacted 72 respondents participated which is 96%. Data were collected using questionnaires. All questions were closed-end questions to fit into quantitative analysis. Findings revealed that user's perception of security had a strong influence the security of electronic health records. Therefore, the study recommended that for effective security controls of electronic health records there must a regular users' training and awareness to create a positive user's perceptions of security.

Keywords: User's perceptions, Electronic health records, Security

1.0 Introduction

In electronic health records management users play an important role in the area of information security as they are required to abide by end-user security policies within their core duties Grassegger, T.; Nedbal, D.(2021). Failure to do so may result in threats and vulnerabilities that can be used to break security either inside or externally. For management to be able to "push" the appropriate incentive "buttons" toward developing effective security practices, it is crucial to identify and assess elements that influence the user's security behavior in order to improve the user's deliberate behavior.

The users of the electronic health records, on the other hand, may have a different view of the issues around the security of information. It is crucial for managers and designers of electronic health record security to understand that users can choose whether or not to abide by security

controls measures. Security breaches associated by human being are influenced by many factors such as poor awareness and individual's own goals, boredom, attitudes, lack of training and lack of risk perceptions, Pollock (2017). Other issues that need to be considered under user's decision on security controls are that, users can be placed into different categories, a user's can be an individual user or a group users, Belanger & Crossler (2011). A users have a different level of responsibility and thus have different needs.

The categories of users and their different needs of access to different types of information systems might impact on the perception of users concerning the issues surrounding security controls in information environment. To users the most significant thing is to finish their duties in the most efficient and effective ways possible. At the same times countermeasures are seen as great obstacles to accomplishing their duties, Furnell et al., (2008), this perception might motivate users to find ways to by-pass the countermeasures. It is anticipated that users who have received any kind of security awareness and training should exhibit higher security behavior than users who did not receive it, Puhakainen & Siponen (2010).

Many studies suggest that user's perceptions of security have influence on securing electronic health records, (Belanger & Crossler 2011; Pollock (2017). However, most of these studies were done in the countries other than Tanzania. Because of this, not much is really known on the case of Tanzania especially in public hospitals. Therefore, to fill this gap, this paper examined the influence of individual perceptions' of security, including psychological, social, cultural aspects, knowledge, attitude and behavior among healthcare users in Tanzania public hospitals.

2.0 OBJECTIVE OF THE STUDY

The main objective of this study was to assess the influence of user's perception of security on security of electronic health records in Tanzania public hospitals

3.0 LITERATURE REVIEW

Theoretical Literature Review

This study was guided by the theory of Planned Behavior (TPB).

Theory of Planned Behavior

Ajzen (1991) framed the seminal theory of planned behavior (TPB), which is one of the most widely used theoretical frameworks for understanding many of the human factors that influence behavioral actions. The TPB emphases on theoretical models that take into account an individual's motivational and cognitive factors as important predictors of variables of whether they will behave or not act behaviorally (Ajzen, 1991). The theory of planned behavior states that the intention to execute an action is the most immediate determinant of the response, and that attitude, subjective norms toward behavior, and perceived behavioral control over the performance of behavior are all significant influences as well (Ajzen, 1991).

Individual ideas about the outcomes of the performance of the conduct have a substantial impact on employee attitudes and perceptions about a behavior when considering information security in the context of TPB (behavioral beliefs). Employees will be more enthusiastic about engaging in a behavior if they think a favorable outcome is what will happen as a result of doing it (Ajzen, 1991). Employees will feel more positive about promoting and participating in the proper actions if they are taught, highly acknowledged and heavily rewarded (Ajzen, 1991). TPB is selected as

theoretical basis for this study because of its applicability with regards to this research topic that is user's perception of security on security of electronic health records in Tanzanian public hospitals.

Empirical Literature Review

According to Pollock (2017), there are several causes of an information security breaches associated to human such lack of users risk perception, lack of training and poor security awareness. Further Hadlington (2018), mentioned the relationship between cyber security attitudes and behaviors of employees. The study mentioned user's perceived behaviors such as the use of the same password for multiple websites, sharing of passwords with colleagues and clicking on links in emails which are active parts of security breaches.

Ifinedo (2012) conducted the study to examine the impact of different user perceptions on information security and examine individual perceptions of societal normative pressures, or that such behavior, also called normative, should not be engaged, beliefs are more important. According to the study, a person's behavioral intentions are positively impacted by relevant beliefs. This is closely related to how users choose what actions to take based on their impressions of other people who are significant to them. The same study concurred that an individual's behavioral intentions were similarly influenced by their view of their capacity to manage and deal with problems (coping appraisal).

Bulgurcu et al. (2010) suggested that user's attitude is contributed by the advantage of compliance, the cost of compliance and cost of non-compliance by the benefit of compliance, the cost of compliance and cost of non-compliance which are beliefs about the overall assessment of consequences of compliance or noncompliance. This study makes the argument that how essential the information is to the user will have a significant impact on how they perceive the

information security measures in a given information system. This significantly affects how well the user complies with security compliances.

A study by Buttement et al. (2018), suggest that users' intentions to act in information security management situations depend primarily on actual and anticipated costs and benefits, and there is a level to which users perceive unexpected costs over benefits, and the level of security procedures. The study suggests on the creation of positive user's perceptions to security controls in order for the users to comply with security issues of electronic health records.

Patel V et al. (2016), Report on trends in individual perceptions of privacy and security when sharing electronic medical records and health information. They found that more than half of people across the country expressed concern about the confidentiality of their medical records: people did not share information with medical staff. Between 2012 and 2014, over 80% of people believed their healthcare providers had taken steps to adequately protect the EHRs.

3.0 METHODOLOGY

This study adopted the quantitative research approach to provide a starting point in understanding the user's perception of security on security of electronic health records in Tanzania public hospitals. Data were collected at Mount Meru Regional Referral hospital in Arusha. Mount Meru referral hospital is a public hospital located in Arusha region northern part of Tanzania. The main reason for choosing Mount Meru referral hospital as area of study is because the hospital have been using different electronic health records systems in their health service delivery for many years, (MOHCDGEC (2017). The target population included IT officers, Medical Doctors, Nurses, Pharmacists, Laboratory assistants, Clinical officers, record officers and administrative staffs working in the public hospitals. Purposive non-probability

sampling technique was applied to select a total number of 75 participants, 72 respondents out 75 which is 96% participated in the study. Based on ethical issues, privacy, and security reasons, the names of participants have not been mentioned in this paper, but ethical clearance was duly obtained from the hospital. Data were collected using questionnaires. All questions were closed-end questions to fit into quantitative analysis. Pearson's correlation, descriptive statistics, and frequencies were used in the analysis and tests.

4.0 FINDINGS AND DISCUSSION

Demographic Characteristics of Respondents

A total of 75 questionnaires was distributed to the subjects under study. The rate of response was very good as 96% of the respondents returned the questionnaire. On the respondents' gender 52.7 percent were male and about 47.3 percent were female. This implies that both genders were sufficiently represented in the study, majority of the respondents (58%) were at the age of 31-40 years; whereas 29% were between 20-30 years, 7% were at the age of 41-50, 6% were at the age between 51-60 years and none were above 60 years. Further, majority of respondents (52.7%) had attained Bachelor degree followed by (29.2%) who were Diploma holder, 9.7% had master degree level of education and 8.3% had certificate as their highest level of education. This implies that the respondents had relevant skills and knowledge in regards to security of electronic health records. On other hand, 38.8% of respondents were nurses, 22.3% were medical doctors, 11.1% were laboratory technologists, 9.7% were record officers and pharmacists respectively and 4.2% were IT officers and administrator respectively.

Table 4.1 Demographics Variables

Variable	Elements of Measurement	Frequency	Percent
Age	20-30 years	21	29
	31-40 years	42	58
	41-50 years	05	07
	51-60 years	04	06
	Above 61 years	00	1.6
	Total	**72**	**100.0**
Gender	Male	38	52.7
	Female	34	47.3
	Total	**190**	**100.0**
Education Level	Certificate	06	8.3
	Diploma	21	29.2
	Bachelor Degree	38	52.7
	Master Degree	07	9.7
	Total	**72**	**100**
Occupation	IT Officers	03	4.2
	Medical Doctors	16	22.3
	Nurses	28	38.8
	Pharmacists	07	9.7
	Lab. Technologists	08	11.1
	Record officers	07	9.7
	Health administrator	03	4.2
	Total	**72**	**100**

Source: Field Data (2022)

Influence of user's perception of security on security of electronic health records

The table 4.2 clearly shows that user's perception of security have the strong influence on the security of electronic health records in Tanzanian public hospitals. This is because the extent on the indicators tested under this objective to respondents portrayed that user's perception of security such as presence of security breaches of EHRs due to lack of users' understanding on security issues, lack of users' training and awareness on security of EHR systems, users' poor attitude on security issues, users feelings that it is not their responsibility, lack of users motivation to participate in security, users' lack of self-interest to deal with security issues in their organization and users' lack of time to deal with security issues of EHRs. The high percentage of agreement and strong agreement on the indicators mentioned above shows that user's perception of security influence the security of electronic health records in public hospitals. This findings is similar to the study conducted by Pollock (2017), which states that the causes of security breaches are lack of users risk perception, lack of training and poor security awareness. Similarly, Hadlington (2018), mentioned that user's behavioral intention such as the use of the same password for multiple websites, sharing of passwords with colleagues and clicking on links in emails which are active parts of security breaches.

Shay et al., (2010) supported this findings as they states that users often lack motivation to use strong password since they are not convinced about the importance of suggestions in the information systems security policy. It is proved that the user's awareness of information systems problems is not adequate to restrain users from undesirable security practices such as sharing and reusing their passwords.

Table 4.2. The influence of user's perception of security on electronic health records

Item	Strongly disagree		Disagree		Neutral		Agree		Strongly agree	
	F	%	F	%	F	%	F	%	F	%
There is security breaches of EHRs as users lack understanding of security issues	8	11.3	10	13.8	9	12.5	22	30.5	23	31.9
There is security breaches of EHRs as users lack awareness on security of EHR systems	8	11.3	19	26.4	2	2.8	28	39.0	15	20.6
There is security breaches of EHRs due to users' poor attitude towards security issues	14	19.4	9	12.5	10	14.0	23	31.9	15	20.6
There is security breaches of EHRs as users feel that security of EHRs is not their responsibility	9	12.5	13	18.0	4	5.5	26	36.2	20	27.8
There is security breaches of EHRs as users lack motivation to participate in security	6	8.3	3	4.2	13	18.1	27	37.5	23	31.9
There is security breaches of EHR as users lack self-interest to deal with security issues in their organization	8	11.3	14	19.4	1	1.4	33	45.7	16	22.2
There is security breaches of EHR as users lack time to deal with security issues of EHRs	10	14.0	20	27.7	3	4.2	23	31.9	16	22.2

Source: Field Data (2022): F= Frequency, N= Total Number of sample

Correlations between user's perception of security and security of electronic health records

In determining the influence of user's perception of security and security of electronic health records in Tanzania public hospitals, correlation analysis was carried out. Pearson correlation coefficient (r) was used to determine the strength of the relationship between user's perception of security and security of electronic health records in Tanzania public hospitals. This is shown in table 4.3 which indicates that there was positive relationship between user's perception of security (0.942) and security and security of electronic health records in Tanzanian public hospitals.

Table 4.3: Correlations between user's perception of security and security of electronic health records in Tanzanian public hospitals.

		EHR security	User's perception of security
EHR security	Pearson Correlation	1	.942
	Sig. (2-tailed)		.000
	N	72	72
User's perception of security	Pearson Correlation	.942	1
	Sig. (2-tailed)	.000	
	N	72	72

Correlation is significant at the 0.01 level (2-tailed).

5.0 CONCLUSION AND RECOMMENDATION

The results of this study has shown that in the hospital there is, lack of users' understanding on security issues, lack of users' training and awareness on security of EHR systems, users' poor attitude on security issues, users feelings that it is not their responsibility, lack of users motivation to participate in security, users' lack of self-interest to deal with security issues and users' lack of time to deal with security issues of EHRs. The findings also indicate that there is a strong relationship between user's perception and security of electronic health records in Tanzanian public hospitals.

This study recommends that in order to have a secured electronic health records systems, the hospital management should put into focus on building a positive user's perception of security risks through frequently training and awareness programs. Further, this study recommends further similar studies to be conducted in other public hospitals.

REFERENCES

Adams, A. and Sasse, A. (1999). “User are not the enemy”, Communications of the ACM, Vol 42 N0.12,pp.41-46.

Abawajy, J. User preference of cyber security awareness delivery methods. Behav. Inf. Technol. 2014, 33, 237–248

Albrechtsen, E. A qualitative study of users’ view on information security. Comput. Secur. 2007, 26, 276–289.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes , 50*(2), 179-211.

Anwar, M.; He, W.; Ash, I.; Yuan, X.; Li, L.; Xu, L. Gender difference and employees’ cybersecurity behaviors. Comput. Hum. Behav. 2017, 69, 437–443.

Belanger, F & Crossler, R.E (2011). “Privacy in the digital age: A review of information privacy research in information systems”, MIS Quarterly, Vol. 35 No. 4 pp.1017-1041.

Beautement, A., Sasse, M.A & Wonham, M (2008). The compliance budget managing security behavior in the organizations” Security.

Furnell, S., Tsaganidi, V & Phippen, A (2008). "Security beliefs and barriers for novice internet users", Computers & security, Elsevier Ltd, Vol. 27 No.7-8,pp. 235-240

Grassegger, T.; Nedbal, D. The Role of Employees’ Information Security Awareness on the Intention to Resist Social Engineering. Procedia Comput. Sci. 2021, 181, 59–66.

Hadlington L., (2018). The Human Factor in cybersecurity: Exploring the Accidental insider, IGIGLOBAL, UK

Ifinedo, P. (2012), “Understanding information systems security policy compliance: integration of

the theory of planned behavior and the protection motivation theory', computers & security, Elsevier ltd, Vol.31 No 1,pp. 83-95.

Leonard L,N & Ccronan T.P; Kreie J. What influences technical behavior intentions, planned behavior reason education, perceived importance or individual characteristics? Inf manag. 2004,42, 143-158

Pahnila, S., Siponen, M & Mahmood, A (2007). "Employees behavior towards IS Security policy

compliance", 40th Hawaii International Conference on system sciences

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. Comput. Secur. 2017, 66, 40–51

Pollock T., (2017). Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS), KSU Proceedings on Cybersecurity Education, Research and practice, Kennesaw State University

Puhakainen, P & Siponen, M (2010), Improving employess compliance through information system security training: an action research stsudy. MIS Quarterly Vol. 34 No. 4, pp. 757-778

Safa, N.S.; Sookhak, M.; Von Solms, R.; Furnell, S.; Ghani, N.A.; Herawan, T. Information security conscious care behaviour formation in organizations. Comput. Secur. 2015, 53, 65–78

Thirumalai, C; Chandhini, S.A; Vaishnavi, M.A (2017). Analyzing the concrete compressive strength using Pearson and Spearman. In Proceedings of the 2017 International Conference of Electronics Communication and Aerospace Technology (ICECA), Coimbatore, India, 20-22 April 2017; IEEE: Piscataway, NJ, USA, 2017; Volume 2, pp.215-218

Uffen, J.; Guhr, N.; Breitner, M.H. Personality Traits and Information Security Management: An Empirical Study of Information Security Executives. In Proceedings of the International Conference on Information Systems, ICIS 2012, Orlando, FL, USA, 16–19 December 2012.