International Journal of Innovation Scientific Research and Review
Vol. 05, Issue, 09, pp.5148-5154, September 2023
Available online at http://www.journalijisr.com
SJIF Impact Factor 2023: 6.599

Research Article

ISSN: 2582-6131

INFLUENCE OF INFORMATION SECURITY AWARENESS ON SECURITY OF ELECTRONIC HEALTH RECORDS IN TANZANIAN PUBLIC HOSPITALS

[1], * Ernest Godson, [2]Deus Ngaruko, PhD, [2]George Oreku, PhD

[1]Dar es Salaam University College of Education, University of Dar es Salaam, Tanzania.
[2]The Open University of Tanzania, P.O BOX 23409, Dar es Salaam, Tanzania.

Received 12th July 2023; Accepted 13th August 2023; Published online 25th September 2023

ABSTRACT

This paper aimed to assess the influence of information security awareness on security of electronic health records (EHRs) in Tanzanian public hospitals. The study was designed using explanatory hypothesis-testing survey with quantitative approach. The study population were public hospitals in Tanzania and sampled six public hospitals from each country zone. The sample included 300 respondents who were a key EHRs users such as medical doctors, IT officers, nurses, pharmacists, laboratory technologists, record officers and administrative officers from the selected public hospitals in Tanzania. Data was collected using online survey questionnaire. The results revealed a positive statistically significant influence of information security awareness (ISA) on Security of EHRs in Tanzanian public hospitals, ($p<0.01$). Based on this finding it was recommended that information security awareness be conducted on regular basis to ensure involvement of all employees in securing Electronic Health Records. Further, the study recommend that the training should be monitored to ensure its effectiveness in meeting the security control goals.

Keywords: Information Security Awareness, Security Controls, Electronic Health Records, Public Hospitals, Tanzania.

INTRODUCTION

Information security controls in healthcare organizations is a major concern due to the social, economic, and psychological consequences of patient's data loss. Consequently, healthcare organizations are constantly striving to safeguard patient's data, investing significant resources in technical safeguards Rajab and Eydgahi (2019). However, focusing solely on technological aspects of information security is insufficient, as information security is a multidisciplinary field where human behaviour plays a crucial role Rajab and Eydgahi, (2019). Users can directly or indirectly contribute to security breaches in electronic health records due to lack of security knowledge, Safa *et al.,* (2019). Approximately half of all information security breaches worldwide are caused by employees' inadequate adherence to organization's information security policies Humaidi and Balakrishnan (2015). User compliance with information security rules and policies depends on their knowledge and understanding of information security rules and policies (Evangelopoulou and Johnson, 2014).

Understanding information security policies and regulations is crucial for all users of information systems in an organization to ensure that security policies are well understood and not misinterpreted. The European Union Agency for Network and Information Security (ENISA) recognized security knowledge and awareness as two of the most significant security challenges in eHealth Liveri and Skouloudi, (2015). According to Safa *et al.,* (2019) insufficient awareness training on information security can lead to inappropriate behaviour by employees when handling information assets in information systems.
Although it is recognized that information security awareness training is vital for implementing security measures, it is not beyond doubt whether a training communicated to employees is both understandable and capable of influencing security controls. Gaunt (2000) and Jaeger (2018) stated that research on information security awareness is still in its infancy stage in developing countries, with much remaining unknown and numerous unexplored areas that is necessary for effective security controls. Srikwan and Jakobsson (2007) question whether a clear message is being conveyed to information system users regarding identity theft, particularly in terms of what actions to take and why they are necessary. Additionally, Bada *et al.,* (2019) stated that many awareness campaigns and educational initiatives aimed at increasing information security awareness have been unsuccessful in producing long-term impacts on employees' information security behaviour, thereby hindering the implementation of adequate security controls.

Although different studies related to security of electronic health records have been conducted in Tanzania (Busagala 2013; Nehemia, 2014; Kajiruga *et al.,* 2015; Kanani, 2016; Freye *et al.,* 2020), there are still insufficient of the studies which have been conducted to explore the influence of information security awareness on the security of electronic health records in Tanzanian public hospitals. Therefore, this study intends to fill the knowledge gap by examining the influence of information security awareness on security of electronic health records in Tanzanian public hospitals. Thus, the study is guided by the null hypothesis which stated that: Ho: Information security awareness *has no significant influence on security of electronic health records in Tanzanian public hospitals.*

LITERATURE REVIEW

Information security awareness is a key tool in reducing privacy and security breaches in health information systems. According to Nasser *et al.,* (2020), lack of information security awareness training led healthcare personnel to become susceptible to phishing attacks because they ignore basic security issues. Due to the high patient-to-staff ratio, especially in developing countries, healthcare providers are frequently overburdened with work, and their work is sometimes

***Corresponding Author: Ernest Godson,**
1Dar es Salaam University College of Education, University of Dar es Salaam, Tanzania.

characterized by emergency situations, which increases their cognitive load and consequently reduces their attentiveness to security controls, Nasser *et al.,* (2020). The study conducted by Argaw *et al.,* (2020) added that building the cyber resilience of a hospital is a mutual responsibility and necessary. Users (clinicians and administrative staff) should receive training on information security controls and practice digital hygiene in their daily work regardless of nature of their responsibilities.

According to the study carried out by Ay (2008) it is important to make an arrangement of curriculums in health education to include the subject of information technologies before and after graduation for electronic health record privacy and security to be maintained efficiently. Healthcare organizations should communicate to their employees about health data privacy policies and procedures, so that they always protect confidentiality, integrity, and availability of patient's information in the hospitals. Paksoy (2018) emphasised that the practice of the standards determined for security and privacy of electronic health records and frequent training delivery is precious in implementing the culture of information security and privacy. Andriole (2014) added that training employees appropriately regarding security policies formulated regulations and procedures empower them to make accurate judgments concerning security controls. If staff members are properly educated on grammatical errors, since phishing emails often include spelling or grammatical errors or are sent from suspicious addresses that resemble the organization being impersonated, they can make the appropriate choice to keep themselves away from it and thus enhance security measures. The study conducted by Kanani (2016) revealed that Tanzanian healthcare providers lacked knowledge and skills related to ICT, including security issues, resulting in inadequate use of ICT facilities to deliver healthcare services. The study also revealed an absence or deficiency of ICT knowledge, skills, and awareness of available trends on ICT in healthcare services, such as electronic health record security issues. This difficulty is a result of limited information about ICT use, Busagala and Kawono (2013a) lack of training and a deficiency of awareness-raising campaigns on the use of ICTs in the health sector leads to an increase in threats and vulnerabilities to the security of stored electronic patient records.

Theoretical Underpinnings

This study was reinforced by the theory of planned behaviour. According to Ong and Chong, (2014), researchers have found more helpful and practical suggestions due to citing the theory of planned behaviour. The studies by (Khan *et al.,* 2011; Ahlan 2015) have utilized the theory of planned behaviour to forecast compliance with information security, information security awareness, and the sharing of knowledge from an individual's behavioural perspective, thereby making the theory of planned behaviour more relevant in explaining how awareness of information security impacts behaviour related to information security.

According to the theory of planned behaviour, the behaviour is influenced by subjective norms, which are the opinions or actions of an individual based on the broader context, including social networks, workplace surroundings, and social behaviours Mishra and Harris (2006). The perceived behavioural control illustrates how individuals are more likely to undertake a particular action or behave in a certain way if they perceive it as simple rather than difficult (Mishra and Harris, 2006). Hence, in EHR systems, workers are more prone to exhibit favourable behaviour in safeguarding electronic health records systems if they perceive it as effortless rather than challenging to accomplish. The theory of planned behaviour argues that attitudes, subjective norms, and perceived behavioural control all impact intentions, which are the basis of motivation to engage in a particular behaviour Safa and Von Solm (2016). Thus, as employees become familiar with information security control techniques through security awareness, they are more likely to participate and behave positively, perceiving it as more accessible than they previously thought before training. Consequently, an employee who receives adequate information security awareness will develop a positive attitude towards security controls in electronic health records and will be more willing to engage in information security control behaviour and vice versa. The theory of planned behaviour in this study exposed that users will feel more positive about promoting and participating in the proper information security actions if they are taught, highly acknowledged and heavily rewarded (Ajzen, 1991). If users lack understanding, have little knowledge in the information security issues particularly information security policies no vested interest and are frustrated in a way strongly that creates a convincing belief that performing a behaviour is negative, the employees will have an adverse attitude towards a behaviour (Ajzen, 1991) and hence will not comply to the security issues in electronic health records systems.

MATERIALS AND METHODS

Research design

This study used pragmatism philosophy and cross-sectional research design. Pragmatism was used as the study aimed to test hypothesis and generalize the results through exploring what genuinely happens in organizations through scientific measurement of individuals and behaviours Halfpenny, (2015). Deductive approach was adopted due to causal relationships between variables being investigated.

Population and Sampling Procedures

The key EHRs users such as medical doctors, IT officers, nurses, pharmacists, laboratory technologists, record officers and administrative staff from the six public hospitals selected from each country zones formed the population of this study. The total population from this category was 1200. A purposive sampling technique was used to select sample from the population. This technique was used to due to its ability to restrict data collection to the intended sample only. The sample size was calculated based on Yamane (1967). In this formula, sample size can be calculated at 3%, 5%, 7% and 10% precision (e) levels. However, the sample size for this study was calculated at precision level of 5% (e = 0.05) as shown below:

$$n = \frac{N}{1+Ne^2}$$

Whereas:

n = Sample size for population.
N = Size of population
e = level of precision (0.05).

According to the above formula, the sample size for this study is: -

$$n = \frac{1200}{1+1200(0.05 \times 0.05)}$$

$$n = \frac{1200}{4}$$

$$n = 300$$

Therefore, the minimum sample size for the study was 300 respondents

Data Collection Procedures

The instrument for data collection was survey questionnaire. The questionnaire was administered through online kobo toolbox. The use of online tool was necessary as researchers collected data in a wide geographical location (i.e., each country zone). Close ended questions were used in order to encourage specific responses from the study participants. Researchers used questionnaire tool as opposed to other data collection instruments due to its flexibility, cost effective and its applicability to a large sample (Kothari, 2004) The questionnaire was prepared and developed, followed by a pilot study aimed at testing the reliability and validity of the tools. This test also ensured the instructions, questions and scale items were clear as stated by Pallant (2005). The sixty (60) copy of questionnaire was distributed to the prospective participants of this study for pilot test, Mugenda and Mugenda (2003) suggested a sample of at least 10% of the sampled population is usually acceptable in a pilot study. The results from the pilot test yield a Cronbach's alpha of 0.827 indicating that the tool was reliable.

Data Processing and Analysis Method

The collected quantitative data was assessed using descriptive statistics including mean, frequency, maximum, minimum values, and standard deviation which was then computed using these scores as indices of central tendency. Each composite was divided into two mean groups, with the low mean range group designated as low security" and the high mean range group as high-security controls. The researchers used SPSS version 25 to undertake descriptive statistics and the multiple linear regression in order to test the study hypothesis.

Table 1: Information security awareness (ISA) Data processing matrix

ISA Variable	10 items	Total Score range 10 – 50	Mean Score(M) interpretation
			If M=10-27 Low; If M=28-50 High
Awareness on policies and development	3 items	Score 3 – 15	If M=1-2.9 Low; 3-5 High
Awareness on phishing and social engineering	3 items	Score 3 – 15	If M=1-2.9 Low; 3-5 High
Awareness on technical measures	2 items	Score 2 – 10	If M=1-2.9 Low; 3-5 High
Awareness on incident response	2 items	Score 2 – 10	If M=1-2.9 Low; 3-5 High

Regression Equation

Model Specification

$$Y = \beta_0 + \beta X_1 + \varepsilon_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Functional Relationship

$$EHRsec = f(APD, APSE, ATM, AIR) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\ldots\ldots\ldots\ldots\ldots.(2)$$

Model

$$EHRsec = \beta_0 + \beta_1 APD + \beta_2 APSE + \beta_3 ATM + \beta_4 AIR + \ \varepsilon_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

Whereby: EHRsec = Security of electronic health records, β0 = Constant Term, β1= Beta coefficients, APD= Awareness of policy and development, APSE= Awareness of phishing and social engineering, ATM= Awareness of technical measures, AIR= Awareness of incident response, ε = Error Term.

Validity and Reliability

Validity

The validity of the study was determined by performing pre testing of the instrument used for data collection. Before beginning of the actual data collection, the pilot test was performed to 60 individuals from the same study populations. The Cronbach's alpha for the pilot test resulted into 0.827 indicating the tool was valid.

Reliability

The study measured reliability of the instrument using Cronbach's alpha. A Cronbach's alpha of 0.70 and above is deemed good, 0.80 and above is better, and 0.90 and above is best. The study therefore accepted a cut-off point of 0.70 and above.

Ethical consideration

When conducting this study all processes and activities were guided by ethical considerations. Among the most important precautions taken is the request for a research permit from all visited hospitals. Other ethical considerations included the confidentiality of the collected data, which was ensured by the researcher's signature on declaration of confidentiality form. In addition, the researchers sought participant consent and kept consent forms as evidence. Further, the sample selection adhered to the principles of gender parity and equal participation.

RESULTS

Demographic Information

The findings indicated that 52.7% of respondents were males whereas 47.3% were females. Further, majority of respondents (40.3%) were at the age group of 20-30 years. Furthermore, 51.7% of respondents had a bachelor's degree level of education. Also, 49% of respondents had more than 5 years of working experience. Moreover, 23.7% of respondents were nurses, 22.7% were medical doctors, 18.7% were pharmacists, 14% were health laboratory technologists, 7% were record officers and 5.3% were administrative staff.

Table 2. Demographic characteristics

Variables	Category	Frequencies	Percentages
Gender	Male	158	52.7
	Female	142	47.3
Age group	20-30	121	40.3
	31-40	112	37.3
	41-50	41	13.7
	51-60	26	8.7
Education Level	Certificate	43	14.3
	Diploma	84	28
	Bachelor degree	155	51.7
	Master degree	18	6.0
	PhD	00	00
Occupations	IT Officers	26	8.7
	Doctors	68	22.7
	Nurses	71	23.7
	Pharmacists	56	18.7
	Lab. Technologists	42	14.0
	Record officers	21	7.0
	Administrative officers	16	5.2
Working Experiences	Less than 1 year	12	4.0
	1-3 years	41	13.7
	1-5 years	100	33.3
	More than 5 years	147	49.0

Correlation Analysis

To establish whether there was any relationship between information security awareness and security of electronic health records, Pearson correlation was done as indicated in Table 3. The results indicated that there was a positive and significant relationship between awareness on security policies and security of EHRs at r= .259, p<.01 significant level, awareness of phishing and social engineering at r= .216, p<.01 significant level. The analysis further shows that there was a positive and significant relationship between awareness on technical security measure and security EHRs at r= .123, p<.01 significant level and awareness on incident response at r=.220, p<.01 significant level.

Table 1: Correlation Analysis Matrix

		1	2	3	4	5
Security controls of EHRs	Pearson Correlation	1				
	Sig.					
Awareness on security policies	Pearson Correlation	.259	1			
	Sig.	.000				
Awareness on phishing	Pearson Correlation	.216	.193	1		
	Sig.	.000	.001			
Awareness on technical measure	Pearson Correlation	.123	.129	.264	1	
	Sig.	.000	.002	.000		
Awareness on incident response	Pearson Correlation	.220	.294	.199	.301	1
	Sig.	.000	.000	.001	.000	

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

Influence of Information Security Awareness Factors on Security of Electronic Health Records

The regression analysis was used to analyses the influence of information security awareness on security of electronic health records in Tanzanian public hospitals. The findings are presented in *Table 4.*

According to the results displayed in Table 4, the value of R^2 is 0.396 which demonstrates that the independent variables that was investigated contribute to 39.6% of security of electronic health records in Tanzanian public hospitals. This indicates that the remaining 60.4% is attributable to other factors that were not investigated in this research.

Table 4: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R^2 Change	F Change	df1	df2	Sig. F Change
1	.631[a]	.398	.396	7.67353	.398	197.161	4	298	.000

a. Predictors: (Constant), awareness of security policies and development, awareness of phishing and social engineering, awareness of technical measure, awareness on incident response

b. Dependent Variable: Security controls of EHRs

As demonstrated in Table 5, the level of significance is 0.000 which is below 0.05 implying that the model is statistically significant where independent variables had an influence on the outcome variable. The value of F=9.516 is greater than p-0.000. This means that the model was significant.

Table 5: ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	3332.275	4	833.069	9.516	.000[b]
	Residual	25824.311	295	87.540		
	Total	29156.587	299			

a. Dependent variable: Security controls of EHRs

b. Predictors: (Constant), Awareness on incident response, Awareness on technical measure, Awareness on policies, Awareness on phishing and social engineering

The finding revealed that holding the predictors variables (Awareness on security policies, awareness on phishing and social engineering, awareness on technical security measures and awareness on incident response) at constant the level of security of EHRs would be 17.48. It was also revealed that when awareness on security policies is increased by a single unit the level of security of EHRs will increase by 0.791, further, when awareness of phishing and social engineering is increased by single unit the security of EHRs increase by 0.594. Furthermore, when awareness on technical security measure is increased by a single unit the level of security of EHRs increase by 0.254 and when awareness on incident response is increased by single unit the level of security of EHRs increase by 0.803.

Table 6: Information Security Awareness determinants of Security of Electronic Health Records

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	17.488	3.729		4.689	.000		
	Awareness of security policies and development	.791	.247	.186	3.202	.002	.889	1.125
	Awareness of phishing and social engineering	.594	.249	.139	2.383	.018	.884	1.131
	Awareness of technical security measure	.254	.268	.054	.951	.032	.924	1.082
	Awareness of incident response	.803	.348	.134	2.309	.022	.892	1.121

a. Dependent Variable: Security of EHRs

DISCUSSION

The study's findings revealed that information security awareness has a significant positive influence on security of electronic health records in Tanzanian public hospitals. The study by Kuo *et al.,* (2021) agree with this result that information security awareness motivates employees to follow information security policies and hence develop adherence to security controls. The studies by (Kritzinger and Solms, 2010; Talib and Furnell, 2010) proposed that hospitals should conduct regular education and training as an awareness raising method to erase the commonly used statement that, the end user is the weakest link in the information security chain in an organization.

Sommestad (2018) was in line with findings that that, employee's information security awareness has a significant and positive influence on security control in an organization. This means that in healthcare environment if users are well trained on adherence with information security policies of particular organization automatically will develop a positive information security behaviour. The study findings in this study were also in consistent with those of (Kuo *et al.,* 2021; Kim, Choi and Han, 2019) who found that, information security awareness programs have a positive influence on security controls as it motivates employees to follow information security policies and procedures. Albrechtse and Hovden (2010) stated that when public hospital's employees get appropriate information security awareness they recognize the significant of information security controls and can suppress the possibility of information infringement while obeying information security norms and policies. In this regard, the education and training in enhancing information security awareness are the most direct and cost-effective means by which employees who are the users can acquire the latest technical information regarding the security controls issue.

The study conducted by Filik and Unalan (2021) was in line with findings of this study, they revealed that, there is a correlation between information security awareness and security of electronic health records. The two structures had a large and significant coefficient ($p<0.001$). This result means that, as the medical secretaries had information security awareness, the electronic health records security privacy standard increased, and the opposite was also true. In other word, this study mentioned that, this situation is a cause-and-effect relation. Paksoy (2019), supported the finding of this study and emphasized that, the practice of the standards determined for the security and privacy of electronic health records and regular training delivery is quite important in adopting the culture of information security and privacy in healthcare organizations.

CONCLUSION AND RECOMMENDATION

The study concluded that information security awareness is significant predictor of security of EHRs in Tanzanian public hospitals. If public hospitals make efforts to ensure information security awareness to all healthcare employees, then security of EHRs will be realized and enhanced. This gives assurance that other factors being constant, the implementation of information security awareness training will continue to enhance involvement of employees in security of EHRs which may results to adequate security controls of EHRs in public hospitals. This study therefore recommends that public hospitals' management, Ministry of Health and other stakeholders in health services should give credit to information security awareness to enhance security controls of patient's information particularly when using electronic health records systems (EHRs). This may also encourage the involvement of all employees to participate in securing patient's information. The future study on information security awareness on security of EHRs should focus on identifying factors that limit hospitals to conduct regular information security awareness training, difficulties, and obstacle. Furthermore, interviews, focus group discussions might be employed to get an in-depth knowledge on the influence of information security awareness on security of electronic health records in Tanzanian public hospitals.

REFERENCES

Argaw Salema, Juan R. Troncoso-Pastoriza, Darren Lacey, Marie-Valentine Florin, Franck Calcavecchia, Denise Anderson, Wayne Burleson, Jan-Michael Vogel, Chana O'Leary, Bruce Eshaya-Chauvin and Antoine Flahault (2020). Cybersecurity of hospitals: discussing the challenges and working toward mitigating the risk. https://doi.org/10.1186/s12911-020-01161-7

Andriole, KP. Security of electronic medical information and patient privacy: what you need to know. Journal of the American College of Radiology 11(12): 1212-1216. 2014

Ahlan. A, M. Lubis and A. Lubis, "Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures", Procedia Computer Science, vol. 72, pp. 361-373, 2015

Ajzen, "The theory of planned behaviour", Organizational Behavior and Human Decision Processes, vol. 50, no. 2, pp. 179-211, 1991.

Ay, F. (2008). Elektronik hasta kayıtları: Güvenlik, etik ve yasal sorunlar. Bilim ve Teknoloji Dergisi, 9(2), 65-175.

Bada. M, A. Sasse, and J. R. C. Nurse, ―Cyber security awareness campaigns: Why do they fail to change behaviour? in International Conference on Cyber Security for Sustainable Society, 2019.

Busagala L. S. P. and Kawono G. C. (2013a). Underlying Challenges of E-Health Adoption in Tanzania. International Journal of Information and Communication Technology Research. Volume 3 No. 1, January. ISSN 2223-4985

Evangelopoulou, C.W. Johnson, "Attack Visualisation for Cyber-Security Situation Awareness", 9th IET International Conference on System Safety and Cyber Security 2014 Oct. 15-16, Manchester, UK,

Filik, T. & Ünalan, D. (2021). The Evaluation of the Effect of the Information Security Awareness Level in Medical Secretaries on the Security and Privacy Implementations of Electronic Health Records. Hacettepe Sağlık İdaresi Dergisi, 24(1), 183-202.

Freye M, Dennis-Kenji Kipker, Ezekiel Rindstone, Doreen Mwamlangala (2020). Strengthening protection of personal data in the health sector: a comparative analysis of the Tanzania and Germany eHealth system Datenschutz and Datensicherheit-DuD June 2020 DOI: 10.1007/S11623-020-1291-3

Humaidi. N and V. Balakrishnan, "Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness", International Journal of Information and Education Technology, vol. 5, no. 4, pp. 311-318, 2015.

Kajirunga A., Kalegele K. (2015). Analysis of Activities and Operations in the Current E-Health Landscape in Tanzania: Focus on Interoperability and Collaboration. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 13, No. 6, June 2015. http://sites.google.com/site/ijcsis/

Kanani G. (2016). Money Matters in Health & Tech: The Road towards E-Health in Tanzania. The Citizen Online Magazines (Monday, November 7, 2016). Retrieved on 08th March. 2019 at https://www.thecitizen.co.tz/magazine/The-road-towards-e-Health-in-Tanzania/1840564-3443772-format-xhtmlnboinv/ index.html

Khan. B, K. Alghathbar, S. Nabi and M. Khan, "Effectiveness of information security awareness methods based on psychological theories", African Journal of Business Management, vol. 5, no. 26, pp. 10862-10868, 2011

Liveri, A. Sarri, C. Skouloudi, "Security and Resilience in eHealth Infrastructures and Services", ENISA Report, ISBN 978-92-9204-137-3, December 2015.

Kim.H, H. Choi and J. Han, "Leader power and employees' information security policy compliance", Security Journal, vol. 32, no. 4, pp. 391409, 2019

Kritzinger, E. and Solms, S. H. von. Cyber security for home users: A new way of protection through awareness enforcement', Computers & Security, 29(8), pp. 840–847. doi: 10.1016/ j.cose.2010.08.001. 2010

Kothari, C (2004). Research Methodology: Methods and Techniques (2nd Ed.). New Delhi: New Age International (P) Limited

Kuo. K, P. Talley and D. Lin, "Hospital Staff's Adherence to Information Security Policy: A Quest for the Antecedents of Deterrence Variables", INQUIRY: The Journal of Health Care Organization, Provision, and Financing, vol. 58, pp. 1-12, 2021

Mishra, S., & Harris, M. A. (2006). Human behavioural aspects in information systems security literature review. Retrieved from https://www.semanticscholar.org/paper/HumanBehavioral-Aspects-in-Information-Systems-Mishra Harris/a74bb1a1c34526128b183f956a50443c5df6d3c0

Mugenda & Mugenda (2003). Research methods: quantitative and qualitative approaches: Africa center for Technology (ACTS), Nairobi Kenya,

Nasser, G.; Morrison, B.W.; Bayl-Smith, P.; Taib, R.; Gayed, M.; Wiggins, M.W (2020). The Role of Cue Utilization and Cognitive

Load in the Recognition of Phishing Emails. Front. Big Data 2020,3,

Nehemiah L, N (2014). Towards EHR interoperability in Tanzania hospitals: issues, challenges and opportunities. International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.4, No.4, August 2014

Safa, C. Maple, S. Furnell, M. A. Azad, C. Perera, M. Dabbagh, and M. Sookhak, "Deterrence and prevention-based model to mitigate information security insider threats in organisations", Future Generation Computer Systems, vol. 97, pp. 587-597, 2019

Ong. L and C. Chong, "Information Security Awareness: An Application of Psychological Factors–A Study in Malaysia", in 2014 International Conference on Computer, Communications and Information Technology (CCIT 2014), 2014, pp. 98-101.

Rajab. M and A. Eydgahi, "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education", Computers &amp; Security, vol. 80, pp. 211-223, 2019

Safa. N, M. Sookhak, R. Von Solms, S. Furnell, N. Ghani and T. Herawan, "Information security conscious care behaviour formation in organizations", Computers & Security, vol. 53, pp. 65-78, 2015. http: 10.1016/j.cose.2015.05.012.

Sommestad. T, "Work-related groups and information security policy compliance", Information & Computer Security, vol. 26, no. 5, pp. 533550, 2018. Available: 10.1108/ics-08-2017-0054

Talib, S., Clarke, N. L. and Furnell, S. M. ‘An analysis of information security awareness within home and work environments’, Institute of Electrical & Electronics Engineers (IEEE). 2010

****