East African Journal of Business and Economics
eajbe.eanso.org
Volume 6, Issue 1, 2023
Print ISSN: 2707-4250 | Online ISSN: 2707-4269
Title DOI: https://doi.org/10.37284/2707-4269

EASO
EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Effects of Continuous Security Monitoring on Security Controls of Electronic Health Records in Public Hospitals, Tanzania

Ernest Godson[1], Deus Dominic Ngaruko[1] & George Oreku[1]*

[1] The Open University of Tanzania, P. O. Box 23409, Dar es Salaam, Tanzania
* Correspondence ORCID ID: https://orcid.org/0009-0008-8792-9096; Email: godsonernest21@gmail.com

Article DOI: https://doi.org/10.37284/eajbe.6.1.1433

Date Published:

14 September 2023

Keywords:

Continuous Security Monitoring, Security Controls, Electronic Health Records, Tanzania

ABSTRACT

This paper examines the effects of continuous security monitoring on the security of electronic health records in Tanzanian public hospitals. The study adopted a cross-sectional research design and quantitative research approach using a sample of 300 respondents from the six public hospitals in Tanzania. A questionnaire was used to collect data from the main users of EHRs such as medical doctors, IT officers, nurses, pharmacists, laboratory technologists, record officers and administrative officers. A multiple linear regression model was used to evaluate the effects of continuous security monitoring on the security of electronic health records in Tanzanian public hospitals. The findings revealed that continuous security monitoring is a significant predictor of the security of electronic health records in Tanzanian public hospitals, (B= .509, p< 0.001). This implies that, continuous security monitoring explains 50.9% of the variance in security of electronic health records in Tanzanian public hospitals. Based on this finding, is recommended that, to enhance effective security controls in electronic health records, public hospitals in Tanzanian should consider the adoption of continuous security monitoring by making security controls more automated.

APA CITATION

Godson, E., Ngaruko, D. D., & Oreku, G. (2023). Effects of Continuous Security Monitoring on Security Controls of Electronic Health Records in Public Hospitals, Tanzania. *East African Journal of Business and Economics*, *6*(1), 364-374. https://doi.org/10.37284/eajbe.6.1.1433

CHICAGO CITATION

Godson, Ernest, Deus Dominic Ngaruko and George Oreku. 2023. "Effects of Continuous Security Monitoring on Security Controls of Electronic Health Records in Public Hospitals, Tanzania". *East African Journal of Business and Economics* 6 (1), 364-374. https://doi.org/10.37284/eajbe.6.1.1433.

HARVARD CITATION

Godson, E., Ngaruko, D. D., & Oreku, G. (2023) "Effects of Continuous Security Monitoring on Security Controls of Electronic Health Records in Public Hospitals, Tanzania", *East African Journal of Business and Economics*, 6(1), pp. 364-374. doi: 10.37284/eajbe.6.1.1433.

IEEE CITATION

E. Godson, D. D. Ngaruko & G. Oreku "Effects of Continuous Security Monitoring on Security Controls of Electronic Health Records in Public Hospitals, Tanzania", *EAJBE*, vol. 6, no. 1, pp. 364-374, Sep. 2023.

MLA CITATION

Godson, Ernest, Deus Dominic Ngaruko & George Oreku. "Effects of Continuous Security Monitoring on Security Controls of Electronic Health Records in Public Hospitals, Tanzania". *East African Journal of Business and Economics,* Vol. 6, no. 1, Sep. 2023, pp. 364-374, doi:10.37284/eajbe.6.1.1433.

INTRODUCTION

The rise in the number and severity of information security breaches and attacks in healthcare organizations has stimulated the need to protect systems against breaches and attacks, Ponemon Institute (2018). Attacks target all aspects of a system from email to web applications to the network backbone infrastructure itself, Microsoft (2018). While hospitals security experts work to stay ahead of the curve, they find themselves competing against attacks and attackers can cause widespread chaos throughout a network with very little work. While attackers of information systems are utilizing automated attacks techniques often, security experts have not heavily invested on continuous security monitoring despite studies which show that continuous security monitoring helps to minimize the frequency and severity of data breaches.

Continuous security monitoring goes beyond appliances which is the point many technical personnel miss out when planning for the techniques to secure their institutions against attackers. Continuous security monitoring provides situational awareness or real-time risk management whereby organizations get to know what is going on regarding risks and vulnerabilities in their organizations, NIST (2000). Organizations also get to know the situation before, during and after attacks when continuous security monitoring exists.

Therefore, healthcare organizations can eliminate some of the possible security dangers through continuous security monitoring as the continuous monitoring of information security processes allows for collecting and aggregating data, correlating information, and making decisions in ways that are not possible for human cyber security experts (AlSadhan& Park,2015). When organization automate the update of antivirus software it does little good for a yet unseen virus. Similarly, when organization automate the update of operating systems it does little to protect things like zero-day vulnerabilities that could potentially take down entire systems. Continuous security monitoring through automation serves two significant purposes, to free the administrator up to do work that is value-adding and needs human interaction and to minimize reaction time between when an event occurs and when a system responds (Kirtley, 2018).

In healthcare settings with a shortage of skilled security professionals, particularly in developing countries, continuous security monitoring through automation will work effectively in analysing and responding to security incidents. Continuous security monitoring can result in higher productivity and can minimize the stress experienced at healthcare organizations hence lead to less burnout. Despite the numerous advantages of continuous security monitoring in information systems, organizations are not taking full advantage of this technology to improve their security capabilities effectively, NIST (2000). This has resulted in attackers getting a more accessible way in their attacks and breaches while security professionals depend on manual systems (2018).

It is evident that, Tanzanian public hospitals extensively have adopted ICT by employing the use of electronic health record systems (MOHCDGEC, 2017). However, little study has been conducted to address ICT's impact on privacy and security issues in EHRs. Thus, there is a lack of enough information on the effects of continuous security monitoring on security controls in electronic health records. This is a silent issue which may harm the privacy and security of individuals and groups during capturing, processing, storage, or transmission of electronic health records. Therefore, the study intends to explore the effects of continuous security monitoring on security controls of electronic health records in Tanzanian public hospitals. Hence, the study aimed to test the hypothesis that: Ho: C*ontinuous security monitoring has no significant effects on security controls of electronic health records in Tanzanian public hospitals.*

LITERATURE REVIEW

According to Yash (2017) continuous security monitoring provides detective controls which are used to oversee and compare access permission concerning current network utilization in order to guarantee that observed actions correspond to the granted authorizations. When inconsistency detected, responsive measures are taken and send alerts to inform the relevant administrators, allowing them to rectify the problem immediately, thereby mitigating any potential risks to the organization. This is a proactive process in risk and vulnerability management in information systems.

Ellen (2019) stated that, continuous security monitoring helps in automatically blocking any events that infringe the organization's security policies, data encryption and other protective activities to prevent end-users from unintentionally or maliciously sharing data that could put the organizations at risk and vulnerabilities. This is very important as many healthcare organizations in developing countries faced lack of experienced and well-trained IT expertise to manage security issues.

According to Jacob (2016) continuous security monitoring through automation process can filter threats to the system, for example, spam filters are designed to scan email automatically. Firewalls block traffic based on its source and direction. The systems can notify system administrators of suspicious traffic or take action against suspicious traffic. For instance, the system may email to the administrator informing him or her of a potential problem, or it may act on its own without human being involvements.

Justin (2019) opines that since organizations sometimes consider external services and remote users which usually are connected in the organizations' network, security administrators need to have continuous security monitoring to monitor what these users are doing to the information systems of an organization. Continuous security monitoring may help to monitor all external services and what users are doing, what devices they are accessing or using, what apps they access and if they are using a virtual private network (VPN) and whether they follow the security policies and procedures of an organization.

According to Petersdide and Butakoy (2015) continuous security monitoring emphasises on the use of automation to give management critical information needed to make cost-effective, risk-based decisions that support adequate security controls. Among functions that are performed through security automation are threat detection, patch management, vulnerability assessment, inventory management, and compliance monitoring and disaster recovery. The primary objective of continuous security monitoring is near real-time risk management by removing unnecessary human elements. Montesino and Fenz (2011) assert that continuous security monitoring techniques through automation perform the task without the need for the user to initiate the security event.

According to Tsai et al., (2018) networking monitoring is a critical concept in the network management as it helps a network administrator to determine the behaviour of a network and the level of safety of its components. The study also added that, continuous monitoring help keep an eye on all events occurring in an organization's network settings through automation hence helping to prevent unauthorized access to the systems or services by identifying intruders and responding to them promptly.

MATERIAL AND METHODS

This paper is based on the quantitative research approach. This approach can be used to identify trends and averages, establish hypothesis, determine causality, and extrapolate results to large populations (Apuke 2017). The explanatory and cross-sectional research design was used as a study's foundation.

The study's population included EHRs users in public hospitals such as hospital IT officers, medical doctors, record officers, pharmacists, health laboratory technologists, nurses and administrative staff. The six public hospitals were purposively selected from the six country zones. The selection of hospitals based on its experiences in the use of EHR systems and the number of patients served per year in a particular zone. The selected hospitals had a target population of 1200. Quantitative data were collected using a questionnaire with the use of Kobo toolbox.

Sample Size and Sampling Techniques

The study employed purposive sampling technique. Sampling is the process of selecting a small subset from the entire population McCall (2018). The purposive sampling was employed to enable researchers to restrict data collection to the targeted respondents only. Sample size for this study was calculated using the formula developed by Yamane (1967). In this formula, sample size can be calculated at 3%, 5%, 7% and 10% precision (e) levels. The sample size for the 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: -

$$n = \frac{1200}{1+1200(0.05 \times 0.05)} = \frac{1200}{4} = 300$$

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

Questionnaire

The study used a survey questionnaire to collect data from respondents. The questionnaire had a close ended questions to encourage specific response. A total of 360 participants from the targeted population was requested to fill out questionnaire. An online data collection tool (Kobo toolbox) was used as data was collected from the broader geographical locations. The total of 300(83%) responses was received. The technique was used to help in avoidance of bias by the researchers; cost-effective way of collecting data, large samples can be contacted easily, and thus the results can be made more dependable and reliable (Kothari, 2004; Cohen et al., 2007; Saunders et al., 2009).

Data Processing and Analysis

The collected quantitative data were assessed using descriptive statistics including frequency, mean, median, mode and standard deviation. An SPSS table was used to display the results. The multiple linear regression analysis was used determine the link between independent variables and outcome variable. This method also allowed researchers to examine the variance of the model together with the proportional contributions of each independent variable to the overall variance.

Table 1: Data processing matrix

Variable	Items	Total Score Range	Mean core (M) Interpretation
	9	**9-45**	**If M=2-25 Moderate; 26-45 Excellent**
Automated measurement	4	4 – 20	If M=1-2.9 Moderate; 3-5 High
Reporting tools and dashboards	3	3 – 15	If M=1-2.9 Moderate; 3-5 High
Alerting and tracking tools	2	2 – 10	If M=1-2.9 Moderate; 3-5 High

Structural Equation

The below model specification guided multiple linear regression analysis

SCEHR= f (CSM) (1)

Whereby, SCEHR= Security Controls of Electronic Health Records, CSM=Continuous Security Monitoring

As stipulated in *Table 1*, continuous security monitoring is a composite score of automated measurement, reporting tools and dashboards and alerting and tracking tools, thus equation 1 may be re-written into equation 2.

$$\text{SCEHR}= f\ (\text{AM, RTD, ATT}) \qquad (2)$$

Structurally, equation 2 can be presented as in equation 3 when an error term is introduced.

$$\text{SCEHR} = \beta_0 + \beta_1\text{AM} + \beta_2\text{RTD} + \beta_3\text{ATT}+ \varepsilon_i \qquad (3)$$

Whereby, SCEHR= Security Controls of Electronic Health Records; β0 = Constant Term; β1= Beta coefficients; AM= Automated measurement; RTD= Reporting tools and dashboards; ATT= Alerting and tracking tools; ε = Error Term

Testing Multiple Linear Regression Assumptions

Before data analysis exercise, researchers tested the assumptions of multiple linear regression analysis. Normality test was performed by developing the normal distribution table and assessed kurtosis and skewness. The finding revealed that, values were within range (i.e., greater, or equal to -2 and less or equal to 2), as suggested by Hair et al. (2010). Researcher also developed and assessed histogram, which also showed that collected data was normally distributed. Linearity test was also performed using the analysis of the graphs produced by the use of SPSS IBM version 25, in which linear correlation was observed between the variables. Thus, the finding revealed that, there was a linear relationship between variables.

Researcher created and analysed scattered plots using SPSS IBM version 25 to test for homoscedasticity as suggested by Hair et al. (2010). The result revealed that, homoscedasticity assumption was met. To test for multicollinearity assumption, the researchers examined variance inflation factor (VIF) and tolerance value. The variance inflation factors (VIF<3) revealed the absence of multicollinearity. Tolerance values were acceptable when ranged between 0 and 1. The condition index indicated that all variables were < 4.

Validity and Reliability

In this study, content validity index (CVI) was used to check validity of the tool. The mean CVI for the study was 0.802, hence the value was higher than 0.70. Constructs validity was maintained by restricting the question to the conceptualization of the variables and ensuring that the metrics for a given variable fit within the same construct. A cronbach's alpha was used to test reliability of the study. The finding revealed that cronbach's alpha was 0.782, 0.747 and 0.832 which is higher than 0.70. Hence, the data was reliable.

Table 2: Summary of Reliability Test

Indicator	Cronbach's alpha	Comments
Automated measurement	0.782	Reliable
Reporting tools and dashboard	0.747	Reliable
Alerting and tracking tools	0.832	Reliable

RESULTS

Sample Description

Under the sample description, five demographic characteristics were assessed; namely gender, age, education level, occupation and working experience (see *Table 3*). The proportion of male and female respondents was almost the same. The highest group was those with the age between 20-30 years who constituted 40%. The finding revealed that more than 50% of respondents had bachelor degree level of education and above. The working experience result indicated that the majority of the participants have been working in the hospitals for more than 5 years. Hence, participants had enough knowledge on security issues on electronic health records.

Table 2: Sample Description

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
	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
	Record officers	21	7
	Administrative officers	16	5.2
Working Experiences	Less than 1 year	12	4
	1-3 years	41	13.7
	1-5 years	100	33.3
	More than 5 years	147	49

Descriptive Statistics Results

The descriptive result revealed that respondents had perception that automated measurement has a moderate effect on security of electronic health records as indicated in *Table 4*. This is apparent from the total composite score mean of automated measurement, which had approximately 9.56 hence fall under the moderate range of 2-25 as formulated in this study (see *Table 4*). This result justifies the need for automated security measures to ensure security of electronic health records. When reporting tools and dashboards assessed, the mean value was 7.19, which fall in the moderate range as established by this study (see *Table 4*). This implies that, respondent had perception that reporting tools and dashboards had moderate effect on the security controls of electronic health records. Moreover, the finding revealed that, alerting and tracking tools had a total mean value of 4.25 indicating that alerting and tracking tools had moderate effect on security of electronic health records. Generally, this finding implies that, continuous security monitoring moderately affects security controls in electronic health records in Tanzanian public hospitals.

Correlation Analysis

The study conducted correlation analysis using Pearson correlation to determine the relationship between two or more variables or datasets in a single group. The result displayed in *Table 5* indicates that all of the correlations were significant at 0.01 significance level. The automated measurement 0.453, reporting tools and dashboards 0.489 and alerting and tracking tools 0.158. Thus, this the result indicates that continuous security monitoring has a positive and statistically significant relationship with security controls of electronic health records in Tanzanian public hospitals. Specifically, this means continuous security monitoring practices have a moderate positive significant effect on security controls of electronic health records.

Table 4: Respondent's composite score measure of central tendency (n=300)

Variable		Mean	Median	Mode	Min	Max	Classification
Automated measurement	AM1	2.39	2.00	1	1	5	Moderate
	AM2	2.51	2.00	1	1	5	Moderate
	AM3	2.33	2.00	1	1	5	Moderate
	AM4	2.34	2.00	1	1	5	Moderate
	Total	9.56	8.00	7.00	4.00	20	Moderate
Reporting tools and dashboards	RTD1	2.21	2.00	2	1	5	Moderate
	RTD2	2.67	2.00	2	1	5	Moderate
	RTD3	2.32	2.00	1	1	5	Moderate
	Total	7.19	6.00	5.00	3.00	15.00	Moderate
Alerting and tracking tools	ATT1	2.32	2.00	1	1	5	Moderate
	ATT2	1.93	2.00	1	1	5	Moderate
	Total	4.25	4.00	2.00	2.00	10.00	Moderate

Table 5: Correlation Analysis

		1	2	3	4
1. Security controls of EHRs	Pearson Correlation	1			
	Sig. (2-tailed)				
2. Automated measurement	Pearson Correlation	.453**	1		
	Sig. (2-tailed)	.000			
3. Reporting tools and dashboards	Pearson Correlation	.489**	.770**	1	
	Sig. (2-tailed)	.000	.000		
4. Alerting and tracking tools	Pearson Correlation	.158**	.095	.051	1
	Sig. (2-tailed)	.006	.101	.380	

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

Regression Analysis

The multiple linear regression analysis was used to determine the effects of continuous security monitoring on the security of electronic health records.

Table 6: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.518	.268	.261	8.49002	.268	36.167	3	296	.000

Predictors: (Constant), Alerting tracking tools, Reporting tools and dashboard, Automated measurement Security controls of EHRs

The coefficient of determination (R^2) indicated in a model summary shows the proportional of the outcome variable variance that can be predicted from the predictor variables. On the other hand, the correlation coefficient (r) shows the strength of the relationship between dependent and independent variables.

The level of significant of each regression coefficient was reported in the study findings and tabulated in *Table 7*, the result shows that both had statistically significant coefficient. A unit increase in automated measurement will account for 40.3% of positive variances in security control of EHRs, while reporting tools and dashboard will account for 24.1% of positive variances in security control of EHRs and alerting and tracking tools will account for 71.1% of positive variances in security control of EHRs.

The study's hypothesised relationship between the independent and dependent variables was subjected to the test. The study hypothesis stated that: **Ho1:** Continuous security monitoring has no effect on security controls of electronic health records in Tanzanian public hospitals". The beta coefficient for the effect of continuous security monitoring on security controls of electronic health records in Tanzanian public hospitals was 0.171, 0.351 and 0.124 and the significance level was p= 0.030, 0.000 and 0.014 respectively. The study rejected the null hypothesis. Therefore, again it can be concluded that continuous security monitoring is statistically significant in affecting security controls of EHRs because all p-values was smaller than the 0.05 limit.

Table 7: Regression analysis coefficient

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	**Std. Err**	**Beta**			**Tolerance**	**VIF**
1	(Constant)	23.967	1.785		13.429	.000		
	Automated measurement	.403	.184	.171	2.186	.030	.404	2.476
	Reporting tools and dashboard	.241	.276	.351	4.494	.000	.406	2.460
	Alerting and tracking tools	.711	.287	.124	2.479	.014	.990	1.010

a. Dependent Variable: Security of EHRs

Outliers, Normality, Linearity and Homoscedasticity Regression Assumptions Testing Results

Figure 1: Histogram for the Standardized Residual of continuous security monitoring

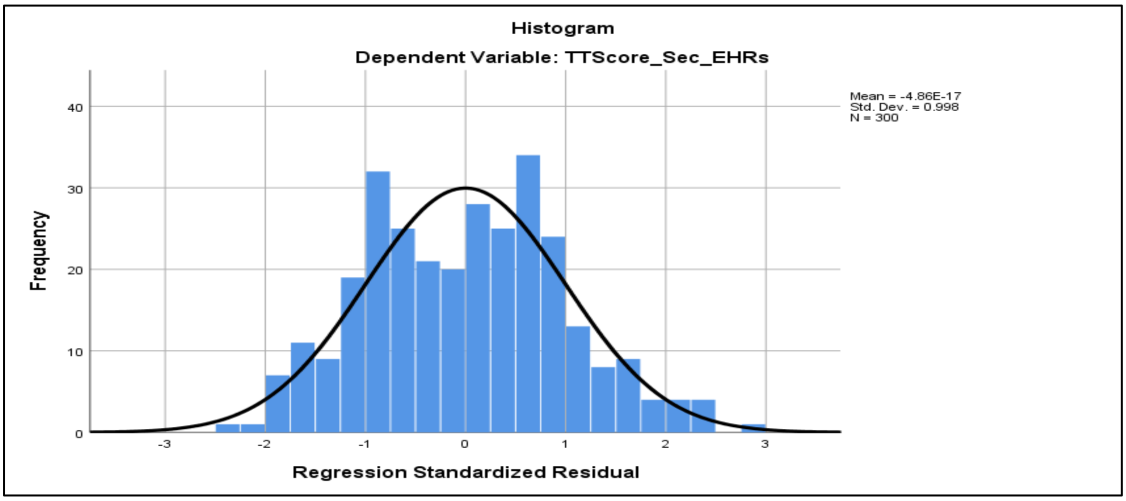


Figure 2: Normal P-Plots for the Standardized Residual of continuous security monitoring

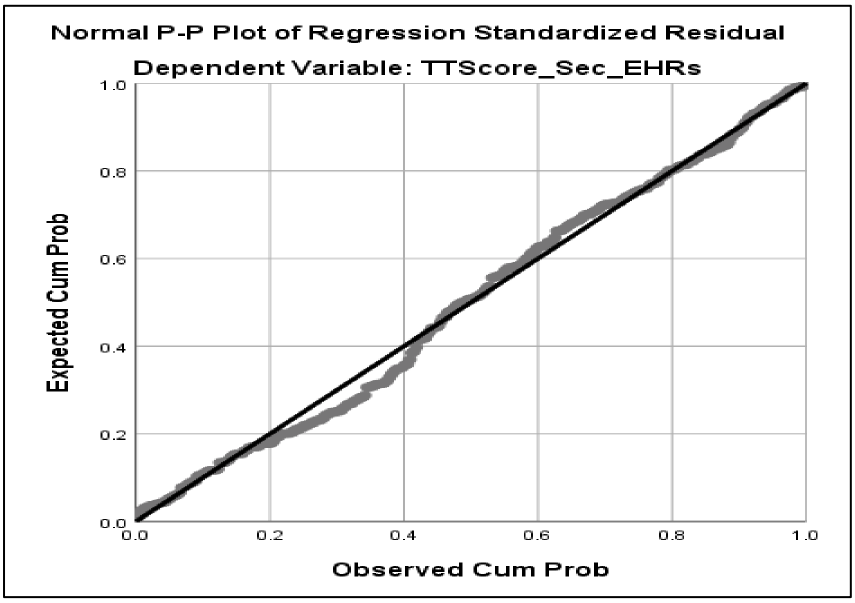
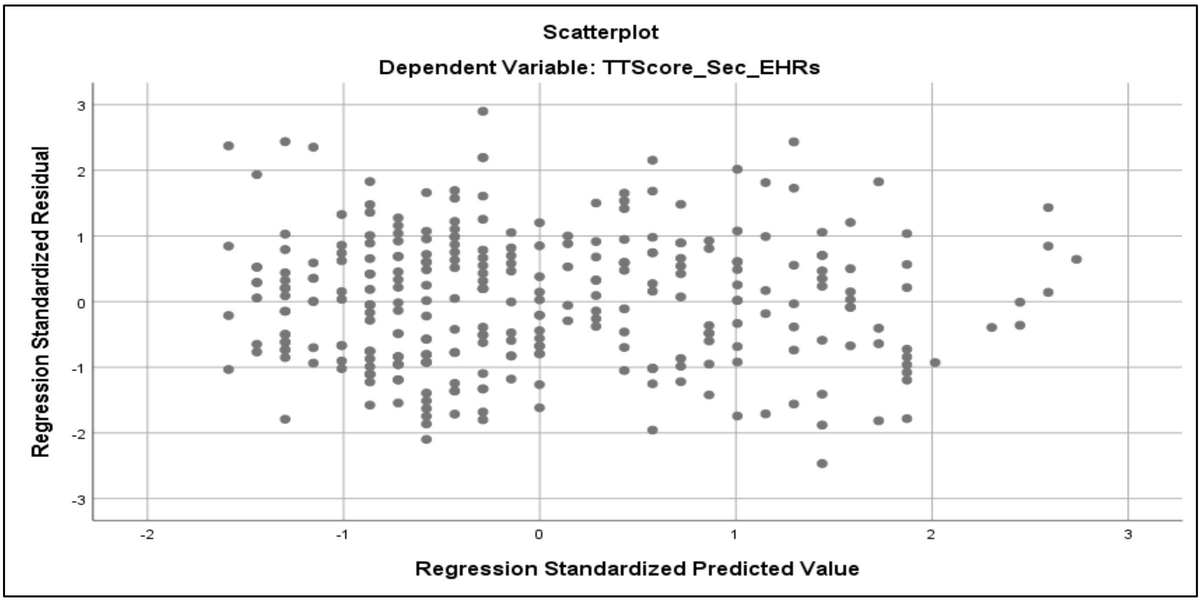


Figure 3: Scatter Plots for the Standardized Residual of continuous security monitoring



DISCUSSION

The results revealed that continuous security monitoring has been agreed to positively affect security controls of electronic health records in Tanzanian public hospitals. This means that having automated measurement, reporting tools and alerting and tracking systems enhance security controls of EHRs in Tanzanian public hospitals. The respondents moderately agreed that continuous security monitoring affect security of EHRs as their response had a mean score of 2.3 to 4.3. The finding is similar to those found by Yash (2017) which reported a significant positive effect between continuous security monitoring practices and security controls in an organization. Abiola & Oyewole (2013) corroborates this finding that monitoring and control activities had positive and significant effects on fraud detection in Nigeria's commercial banks with a P- value of 0.000, 0.005, 0.005, 0.000 and 0.004. Despite the fact that this finding were obtained in banking industry, it can be related to the healthcare industry as patient's information is sensitive as the personal data in the banking industry.

The study conducted by Ellen (2019) was also in line with findings of this study that continuous monitoring has positive effects on the security controls as it helps to automatically block any events that infringe the organizations security policies, data encryption and other protective activities. The respondents agreed that public hospitals had continuous security monitoring however, low level of continuous security monitoring was identified. They insisted on improving security automation, reporting tools and alerting and tracking tools for proper security controls in electronic health record systems. The study found that continuous security monitoring influence security controls of EHRs in a positive significant way, the effects was up to 26.8% hence, effective mechanisms for ensuring continuous security monitoring should not underestimated.

CONCLUSION AND RECOMMENDATIONS

Based on the findings, this paper concludes that continuous security monitoring has a positive and significant effect on the security controls of electronic health records in Tanzanian public hospitals. The Tanzanian public hospitals still have low level of continuous security monitoring due low level of technologies employed in the hospitals. When there is strengthens in continuous security monitoring security controls of electronic health records can be ensured to be effective for more than 25%.

It is therefore recommended that public hospitals should improve its investment on continuous security monitoring practices by the use of automation techniques like antivirus software, intrusion detection and intrusion prevention systems, window firewalls, file encryption, biometrics, audit trail log. The hospitals should combine automatic tools because these tools have different capabilities; for example, intrusion prevention system (IPS) can detect and identify attacks that a firewall and antivirus software cannot detect.

The public hospitals should allocate enough budget for continuous security monitoring including budget for automated infrastructure, regular staff training and awareness on different automated tools. Further, the hospital management should increasingly and continuously pursue standards and procedures that ensure continuous security monitoring are not compromised with budget availability to ensure security controls is achieved on electronic health records.

This study revealed that continuous security monitoring affect security control of EHRs in Tanzanian public hospitals with other factors, the future study can be conducted to focus on other factors which affect security of EHRs and its significant on security controls of EHRs. Similarly, the future studies can focus on both private and public hospitals to get a broader perspective of the subject under the study.

REFERENCES

Abiola, I., & Oyewole, A. T. (2013). Internal control system on fraud detection: Nigeria experience. *Journal of Accounting and Finance*, *13*(5), 141-152.

Apuke, O.D. (2017). Quantitative research methods: A synopsis approach. Kuwait Chapter of Arabian Journal of Business and Management Review, 33(5471), 1-8

AlSadhan. T and J.S. Park, "Leveraging information security continuous monitoring for cyber defence", Proceedings of the 10th International Conference on Cyber Warfare and Security, pp. 401, March 2015.

Ellen Z (2019). What is data loss prevention (DLP)? A definition of data loss prevention. Available at:https//digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

Hair, J. F, Babin, J. B., Anderson, R.E. & Black, C.W. (2010). Multivariate data analysis. (7th edition). Upper Saddle River: Pearson Prentice Hall.

Jacobs, S. (2016). Engineering Information Security. Hoboken: Jacobs.

Article DOI: https://doi.org/10.37284/eajbe.6.1.1433

Justin B (2019). How to gain security visibility into a modern environment, Available at: https://blog.rapid7.com/2019/03/27/hw-to-gain-security-visibility-into-a-modern-environment/ [Assessed on 16 March 2023]

Kirtley, E. (2018). What is SIEM? What is SOAR? How are they different? Retrieved from Swimlane: https://swimlane.com/blog/siem-soar/

Microsoft. (2018, May 30). Task Scheduler - Windows application. Retrieved from Microsoft Docs: https://docs.microsoft.com/en-us/windows/desktop/taskschd/task-scheduler-startpage

MOHCDGEC (2017). Tanzania digital health investment road map 2017-2023: The journey to better data for better health in Tanzania. https://www.healthdatacollaborative.org/where-we- work/Tanzania/; [accessed on 16 Jun. 2021]

Montesino, R., & Fenz, S. (2011). Automation possibilities in information security management. 2011 European Intelligence and Security Informatics Conference

Petersdide, G. B., Zavarsky, P., & Butakov, S. (2015). Automated security configuration checklist for a Cisco IPSec VPN router using SCAP 1.2. The 10th International Conference for Internet Technology and Secured Transactions, 355-360

Ponemon Institute. (2018). 2018 Cost of a Data Breach Study: Global Overview. Traverse City, MI: IBM Security and Ponemon Institute, LLC.

Tabachnick, B.G., & Fidell, L.S. (2014). Using multivariate statistics. Harlow. Essex: Pearson Education Limited

Tsai P-W, Tsai C-W, Hsu C-W, Yang C-S (2018). Network monitoring in software-defined networking: a review. IEEE Syst J. https://doi.org/10.1109/JSYST.2018.2798060

Yash P, (2017). How automating SOD controls monitoring and management strengthens compliance and security. Available at: https://saviynt.com/blog/how-automating-sod-controls-monitoring-and-management-strngtherns-compliance-and-security [Assessed on 06 May 2023]