An Investigation on the Influence of Emerging Cyber-Technologies on the Integrity of Information Systems in Healthcare Facilities.

Jacob Bore, Dr. Collins Ondiek, Dr. James Ogalo

borejac.k@gmail.com
Kisii University,Kisii-40200,Kenya
United States International University-Africa, Nairob-00800i, Kenya

Abstract

Healthcare technology is continually changing and hospitals that want to keep up must be acquitted with new technologies that maintain integrity. The urge in system users to sell patients information puts the integrity of the information systems in question and hence a problem arises in cases where trustworthy staff do not want to utilize these systems in ther service due to the possible data leakages. The Moi Teaching and Referral Hospital was the location of the research. The total participants of the study were 161 members of the MTRH. The Cochran model was used as the sample size formula before the data was analyzed using 12 Likert scale questions and Cronbach's Alpha. The findings showed that the respondents agree that misleading and deceiving system messages and alerts negatively impact system integrity. This study concluded that a statistically significant relationship exists between cybersecurity and customer satisfaction with the system; hence, improving system security improves customer satisfaction. The study recommended that since cybersecurity affects the integrity of the information system at the hospital, the management should ensure well identification and authentication techniques such as IDs and passwords are in place to identify system users and confirm that information is from a trusted source.

Keywords: Information technology, Best Practice, Information and Communications Technology (ICT), Utilization, ICT Adoption, Integrity.

INTRODUCTION

1.1 Background of the Study

Although companies who followed the old rules were among the most successful competitors of their day, the nature of competition has changed in some way since then. Others argue that consumer preferences have shifted, making personalized things more enticing. While historians suggest that the taste for mass-marketed goods had to be established in the early days of mass production, today has increased wealth, and social inequality may make this more difficult (Zarour et al., 20o21). It is also possible to claim that some new emergent cyber technologies were just as useful fifty years ago as they are now but had not been found.

These drastic and dramatic developments have affected the manager's working style; as a result, management procedures require speed, precision, and a picture of the business status via applicable information technology. Mishra et al. (2020) argue that health care is not exceptional; healthcare technology is continually changing; hospitals that want to keep up must be acquitted with new technologies and try to incorporate them into providing quality healthcare. Information technology has enabled the convergence of health technology, digital media, and mobile devices. It is a potential answer to many of the health sector's difficulties, particularly in enabling more effective care integration. Since then, the technological world has changed at a breakneck pace. With the changes, the integrity question rises. This paper analyzed the influence of emerging cyber technologies on the integrity of information systems in healthcare facilities.

1.2 Problem Statement

There are past cases of patient's information leaking or being shared intentionally with third parties by system users hence compromising the integrity of the information systems. Emerging technologies are developed with the guide of data analytics where the data used are majorly stolen or bought from other parties. Therefore, the urge in system users to sell these information puts the integrity of the information systems in question. Therefore, the problem arises in cases where trustworthy staff do not want to utilize these systems in their service due to the possible data leakages.

1.3 Objectives of the Study

To investigate the influence of emerging cyber technologies on the integrity of information systems in healthcare facilities.

1.4 Research Questions

What is the influence of emerging cyber technologies on the integrity of information systems in healthcare facilities?

1.5 Scope of the Study

The study investigated the influence of emerging cyber technologies on the integrity of information systems in healthcare facilities. The focus was on how healthcare can improve with technology to curb mistrust and maintain its integrity in service delivery.

1.6 Significance of the Study

The study's finding is significant in analyzing cyber technologies in keeping the integrity of information in health facilities, for the case of Moi Teaching and Referral Hospital (MTRH). The feedback will be essential in finding ways healthcare can save patients' information while maintaining their integrity. This study will help hospitals make better decisions regarding patients' data and hospital records.

LITERATURE REVIEW

2.1 Introduction

This study aimed to examine the influence of emerging cyber technologies on the integrity of information systems in healthcare facilities. This chapter focused on the literature review on the integrity of information systems by examining deceiving messages and faulty machines.

2.2 Literature Review on Integrity of information systems

The dependability and trustworthiness of information are referred to as information integrity. It is the accuracy, consistency, and dependability of the information content, processes, and systems. Information integrity remains a high priority in organisations' information system applications (Shull, 2019). Any new technology should address integrity issues at all information access levels. Therefore, the emerging technology should prioritize any integrity issues of the system, enhance the high security of information in the system, and prevent unauthorized access.

Threats to organizations can be classified into four categories: motives, resources, accessibility, and technical capacity (Warren, 2018). Various hazards may offer different levels of risk to an organization depending on these components, necessitating different mitigation and prevention tactics; thus, this study seeks to know how this aspect has been addressed and how it is affecting system usage in MTRH. Information Integrity, which necessitates engineering for effective information systems, is primarily concerned with ways of developing cost-effective systems that give operationally effective protection from undesirable events. (Moses, 2018).

2.2.1 Deceiving Messages

Due to the current pandemic integrity of information in healthcare systems has been affected by expanded phishing sites. There have been hacking activities on health institutions' information systems and websites that cybercriminals are using to give false health information and pandemic data, which prompted the WHO to put out an advance notice to the overall population to be more cautious (Argaw et al., 2020). There have been Covid-related spaces that accounted for more than 4000 deceiving messages (i.e., areas that contain words like "crown" or "Coronavirus") have been enrolled since the start of 2020. These enlisted spaces resulted from weakened cybersecurity systems and were used by foes for phishing-related exercises. The attacks have negatively affected the integrity of most healthcare information systems, and some have had to be redeployed.

2.2.2 Deceiving and Faulty Machines

The quick development of artificial intelligence (AI) applications and information investigation in medication are additionally of incredible worry for network safety. Given that AI is material to clinical data innovation frameworks, antagonistic learning - a high-level hostile procedure is intended to trick models. Late investigations in the field of ill-disposed learning have shown effective assaults on clinical gadgets, for example, imaging innovation. Against this backdrop, the integrity of information of the health pandemic systems is affected. In a period of computerized change in medical services, digital dangers are unavoidable, and viable network safety requires a significant interest in foundation, workforce, and administration. (Argaw et al., 2020). With this, the integrity of information of the health pandemic systems is affected.

2.3 Conclusion

This chapter focused on the scholarly reviews on integrity and majorly focused on the deceiving messages and fault machines that force integrity questions to be raised.

METHODOLOGY

3.1 Research Design

A case study research approach was used for the investigation. A case study methodology was used for this research. A research design known as the case study design is used if it is necessary to ascertain facts on the standing of a person or an item. It was used to define what is present in terms of the circumstances or factors in a certain scenario. In early and exploratory research, case studies are used to acquire information, synthesize it, present it, and analyze it without further explanation. Eldoret's Moi Teaching and Referral Hospital (MTRH) was selected to serve as the case for this investigation. Because the nature of the issue as it is now conceived is identical to the condition in MTRH at the time of the research, this design is appropriate for the investigation.

3.2 Locality and Beneficiaries of the Project

The Moi Teaching and Referral Hospital was the location of the research that was carried out. The Moi Teaching and Referral Hospital, more often known as MTRH, is the second National Referral Hospital in Kenya. It may be found in the Rift Valley Province of Kenya, specifically in Eldoret. In 1917, it first served the community as a cottage hospital. After the founding of Moi University in 1984 and the subsequent founding of the Faculty of Health Sciences at the University, the hospital transitioned from a district hospital to an institution that teaches and serves as a referral center. Patients come to be treated at this facility from western Kenya, several regions in eastern Uganda, and southern Sudan. The hospital has a capacity of 800 beds. The AMPATH Centre is associated with the MTRH, and the personnel often collaborates.

3.3 Research Approach

The research approach used here was the qualitative research design. The study was geared towards investigating what leads to cyber-attacks. The findings were important in formulating recommendations to guide the critical health care, stakeholders toward reversing this norm.

3.4 Population and Survey Sampling

3.4.1 Target Population

The target population is the entire group a researcher is interested in (Mugenda &Mugenda (2003). The target population for the current study was 161 staff working at Moi Teaching and Referral Hospital (MTRH). These comprise 18 directors, 63 heads of departments, and 80 ICT staff totaling 161 respondents.

3.4.2 Survey Sampling

The sample size was determined using the A formula propounded by Cochran (1963) was used to determine the sample size was 114 respondents.

3.5 Data Collection Methods

The researcher obtained permission from the National Commission for Science, Technology, and Innovation after receiving an introduction letter from Kisii University, which was presented after the School of Post Graduate Studies supported the idea (NACOSTI). After obtaining the study authorization, the researcher went to the Chief Executive Officer of MTRH to request permission to gather data from the institution. In addition to this, the researcher used the assistance of two study assistants in the distribution of the questionnaires. The researcher went ahead and conducted interviews with important informants.

3.6 Data Analysis

12 Likert scale questions were rolled out to measure Integrity and Availability. Cronbach's Alpha was implemented. Cronbach's Alpha ranges between 0 and 1, with higher values indicating that the questionnaire was more reliable in measuring the intended metric to determine the internal consistency of the 12 questions on integrity.

RESEARCH FINDINGS AND ANALYSIS

4.1 Response Rate

This study obtained a response rate of 74%, which accounted for 76 questionnaires that were dully filled with 102 issued. Mugenda &Mugenda (2003) argue that the statistically significant analysis response rate should be at least 55%.

4.2 Demographics Results

This section provides various demographic information of the respondents, including gender, age, numbers of years worked, education level, department, position at work, knowledge of emerging cybersecurity, and their impact on system integrity.

4.3 Results on the influence of emerging cybersecurity technologies on the integrity of information systems at Moi Teaching and Referral Hospital.

The findings presented in Table 4.11 below highlight the respondents' feedback on the influence of emerging cybersecurity technologies on the integrity of information systems at Moi Teaching and Referral Hospital. The responses were tabulated in means and standard deviations, derived from a Likert Scale of 1-5, where; 1= strongly disagree, 2= disagree, 3= neutral, 4= agree, and 5= strongly agree. A low standard deviation means that the data was clustered around the mean, and a higher standard deviation means that the data had a lot of variability around the mean (widely spread).

The findings revealed that the respondents agree that change in system security gives false messages if not well integrated with hospital workflows with a mean = 3.76 and SD = 1.07. The findings showed that the respondents agree that misleading and deceiving system messages and alerts negatively impact system integrity with a mean = of 4.04 and SD = 0.96. The findings revealed that cyber security impacts customer satisfaction with the system with a mean = 4.10 and SD = 0.83.

The findings also revealed that the respondents agreed that improving system security improves customer satisfaction with a mean= of 4.19 and SD = 0.82. The results revealed that the respondents agreed that frequent changes in system security design/ technology negatively affect staff and customer system satisfaction with a mean = 3.89 and SD = 1.03. The respondents also agreed that changing the information security system would make the organization modify how information is accessed with a mean = 4.04 and SD = 0.88. The findings revealed that the respondents agreed that there is a great difference in how information is accessed in hospital systems due to different security systems deployed with a mean = of 4.07 and SD = 0.83.

The findings revealed that the respondents agreed that information system security plays a key role in facility protection with a mean = of 4.26 and SD = 0.79. The findings also revealed that the respondents agreed that entire facility security is compromised if proper cyber security technology is not in place, with a mean = 4.32 and SD = 0.71.

DISCUSSION CONCLUSION AND RECOMMENDATIONS

5.1 Discussion

The influence of emerging cybersecurity technologies on the integrity of information systems at Moi Teaching and Referral Hospital. This study sought to determine the influence of emerging cybersecurity technologies on the integrity of information systems at Moi Teaching and Referral Hospital. The findings revealed that change in system security gives false messages if not well integrated with hospital workflows and that misleading and deceiving system messages and alerts negatively influence system integrity at a mean of 4.04. The findings agree with Argaw et al. (2020) sought to determine the impact of cybercrime on the integrity of health information systems during the COVID pandemic. Argaw et al. (2020) found out that there have been hacking activities on health institutions' information systems and websites that cybercriminals are using to give false health information and pandemic data, which prompted the WHO to put out an advance

notice to the overall population to be more cautious. The researcher noted that the attacks negatively affected the integrity of most healthcare information systems, and some have had to be redeployed.

5.2 Conclusion

This study concludes that a statistically significant relationship exists between cybersecurity and customer satisfaction with the system; hence, improving system security improves customer satisfaction. The integrity of information systems is essential in determining how information is accessed in hospital systems when different security systems are deployed, which in turn enhances the rate of information system acceptance and adoption. Integrity is essential in creating and designing information systems as it guarantees user security and satisfaction.

5.3 Recommendations

The study recommends that since cybersecurity affects the integrity of the information system at the hospital, the management should ensure well identification and authentication techniques such as IDs and passwords are in place to identify system users and confirm that information is from a trusted source. Robust identification and authentication techniques are important to the hospital because they collect sensitive data from various sources. ICT management should ensure that passwords and access codes frequently change to prevent unauthorized users from breaking into systems, thus lowering the integrity of the information system. Since this study found a relationship between cybersecurity and information system integrity, it recommends that the hospital ensure that any new cybersecurity technology implemented is well integrated with hospital workflows to improve information system integrity.

5.4 Future work

More studies should be done on cyber security trends and how hospitals can be part of the changing trends. MTRH has set the strategic plans that best suit the facilities' implementation technology. Nonetheless, the confidentiality of patients is questioned. Scholars should review more and write more about cyber security so that is the hospitals become dot.com, and patients and healthcare professionals should appreciate the integrity of healthcare.

Appendix

Variable	N	Mean	Std. Deviation
Deceiving messages Cyber security bridge gives deceiving system messages to users in your organization	72	3.40	1.10
Change is system security gives false messages if not well integrated with hospital workflows	72	3.76	1.07
Misleading and deceiving system messages and alerts negatively impact system integrity	72	4.04	0.96
Customer Satisfaction Cyber security has an impact on customer satisfaction with the system	72	4.10	0.83

Improving system security improves customer satisfaction Frequent changes in system security design/ technology affect staff and customer system satisfaction	72	4.19	0.82
	72	3.89	1.03
Modification of Information Cyber security contributes to high information modification Changes in the information security system will make the organization modify how information is accessed There is a great difference in the way information is accessed in hospital systems due to different security systems deployed	72	3.68	1.06
	72	4.04	0.88
	72	4.07	0.83
Protection of the facility Information system security plays a key role in facility protection Entire facility security is compromised if proper cyber security technology is not in place Changes in the information system security interfere with the entire protection of your organization	72	4.26	0.79
	72	4.32	0.71
	72	3.96	0.956

Table 4.11 results on the influence of emerging cybersecurity technologies on the integrity of information systems: Mean of above 3.5= agree and below 3.5=disagree; lower St. Deviation mean less variability

Figure 4.12 below shows the distribution of the total score for integrity for the 12-Likert scale questionnaire. We observed that most respondents believed that the emergence of new cybersecurity technologies would impact the integrity of the information systems.

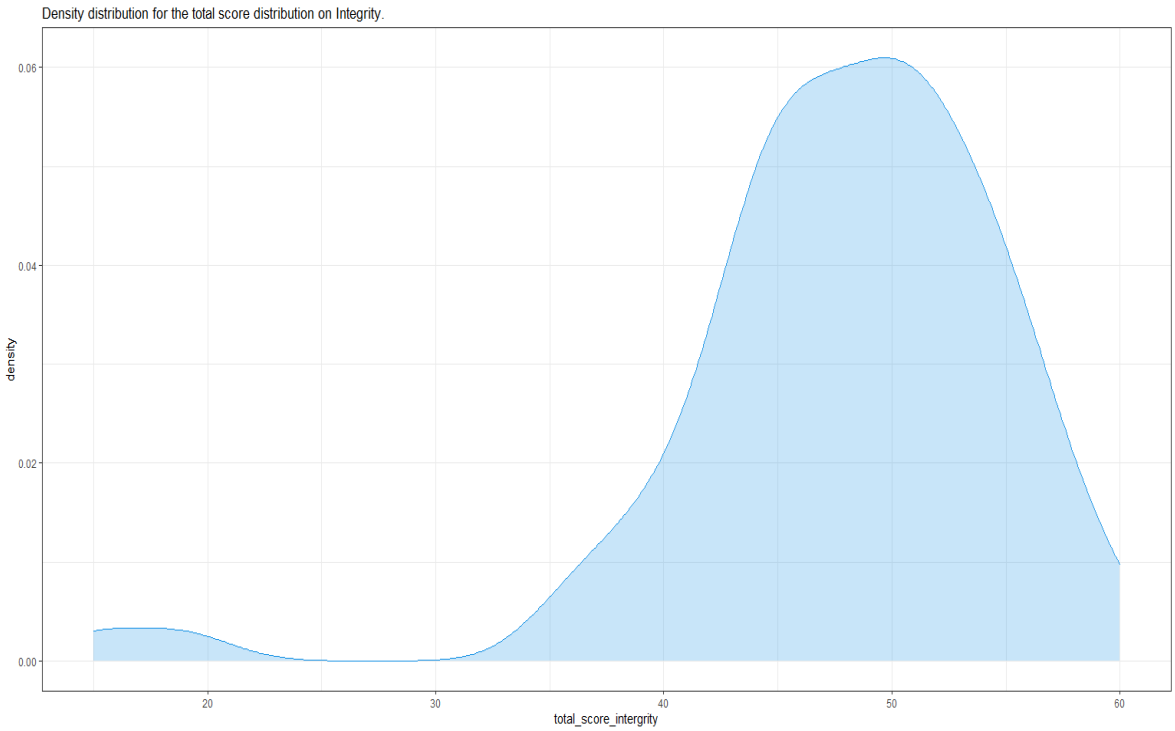

Figure 4.12: Distribution of the total score on integrity.

References

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*(1), 1-10.

Kamary, J. R. (2018). *Cyber Technology And Insecurity In Africa: A Case Study Of Kenya* (Doctoral dissertation, University of Nairobi).

Mishra, S., Alowaidi, M. A., & Sharma, S. K. (2021). Impact of security standards and policies on the credibility of e-government. *Journal of Ambient Intelligence and Humanized Computing*, 1-12.

Moses, G. (2018). *Emerging trends in Information System.* Michigan: McGraw Hill.

Mugenda, O. (2003). &Mugenda A.(2003). *Research methods: quantitative and qualitative approaches.*

Shull, J. G. (2019). Digital health and the state of interoperable electronic health records. *JMIR medical informatics*, *7*(4), e12712.

1. Warren, E. (2018). *Legal, Ethical, and Professional Issues in Information Security.* Washington: Cengage Learning

Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., ... & Khan, R. A. (2021). Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters*, *8*(3), 66-77.