Assessment of ICT infrastructure security vulnerabilities based on confidentiality, integrity, and availability of information

Dismas G. Hiza[1], Pamela Chogo[2]

[1] Kahama Shinyanga Water Supply & Sanitation Authority, Tanzania (hizadismas@gmail.com)

[2] The Institute of Accountancy Arusha, Tanzania (pamsekela@gmail.com)

Abstract

The purpose of the article is to assess the weaknesses of Information and Communication Technology infrastructure security in Tanzania's public sector based on confidentiality, integrity, and availability of information to establish security controls. The vulnerabilities detected were exploited to find out the attacks which could gain successfully unauthorised access through them. Finally, security controls against vulnerabilities were recommended. Data collected from 107 respondents of two public sector organisations were analysed, and results showed the presence of Information and Communication Technology infrastructure vulnerabilities which required strong security controls for fixing them. On the other side, Practical Penetration Testing was conducted to get data which are relevant data about Information and Communication Technology infrastructure security weaknesses. Likewise, the penetration testing results indicated the presence of vulnerabilities. The obtained results were useful in recommending security controls to be established.

Keywords: Vulnerabilities, security controls, confidentiality, integrity, availability

1. INTRODUCTION

Although information technology offers an abundance of advantages, if it is not adequately regulated, it may leave information systems open to security risks such as fraud, sabotage, and other forms of criminal activity (Zhang et al., 2018). There is a problem with establishing strong security controls to protect ICT infrastructure in Tanzania's public sector. Since there is Industrial Revolution Technology for a sustainable National Economy, it is obvious that the security threats index level of information also grows. Insufficient cybersecurity specialists in Tanzania is the main reason for poor preventive measures against security threats (cyberattacks) in the public sector ICT infrastructure. This results in a violation of information confidentiality, integrity, and availability. Thus, the statistics of the security threats index in Tanzania cannot be maintained at the minimal possible level.

ICT infrastructure security vulnerabilities must always be monitored, detected, and fixed to preserve the confidentiality, integrity, and availability of information. According to Khando et al., (2021), Preserving the confidentiality, integrity and availability of an organisation's sensitive information systems assets against attacks and threats is a challenge in this digital age.

Due to automation of most of the public sector operations, there is an increase of cybercrimes which jeopardise the security of sensitive information in Tanzania public sector organisations by violating its confidentiality, integrity and availability. Some sensitive public sector documents have been found on social networks. This means confidentiality as the principle of CIA triad has been violated since unauthorized users can view the documents. Twitter (2022) published a confidential letter about Tanzania ruling party. This means, user who posted it violated confidentiality of information, possibly unknowingly due to lack of cybersecurity basic knowledge.

The leakage of these documents might be caused by unauthorized access to public sector systems, which may also result to altering of information (ie. Violation of Integrity principle of CIA triad). However, there is time to time outage of public sector services such as internet service. It is a normal thing for the customers or users to be informed on unavailability of services due to internet or internal server downtime (ie. Violation of Availability principle of CIA triad).

The Global Economy (2022) published statics for Tanzania Security threat index from 2007 to 2022 shows the average value for Tanzania is 5.44 index points with a minimum of 4.9 index points in 2022 and a maximum of 5.8 index points in 2012. The latest value from 2022 is 4.9 index points. For comparison, the world average in 2022 based on 177 countries is 5.09 index points. The above statistics considers 0 (low) and 10 (high).

Therefore, as per above statistics, it seems there are still some vulnerabilities which result to violation of confidentiality, integrity and availability of information. Hence, the research was carried out to find out ICT vulnerabilities in public sector organisations based on CIA triad Security Model, and finally recommend on possible solutions and preventive measures.

The main objective of the study was to assess the significance of CIA triad Security Model in establishing ICT security controls.

The findings of the study help to establish remarkable security controls based on confidentiality, integrity and availability of information. The sources of vulnerabilities were recognized, then a way for fixing them, and preventive measures were suggested to avoid or minimize possibilities of cyber-attacks such as Payload attacks and Denial of Service (DOS) in future.

2. LITERATURE REVIEW

2.1 General Deterrence Theory

Cordella & Paletti (2018) noted that this theory proposes that people may be stopped from conducting irregular selfish behaviours by the deployment of defensive measures which comprise strong deterrents and consequences compared to the act. This theory relates to assessing ICT infrastructure security vulnerabilities in such a way that, it emphasizes the deployment of defensive measures, which also need to be implemented on ICT infrastructure as security controls according to vulnerabilities observed. Therefore, when leveraging 4th industrial revolution technology, we must pay attention to establishing security controls against vulnerabilities which may arise due to technological growth.

2.2 Game Theory

Games theory presents multi-person choice situations as games where each player selects actions which culminate in the highest potential rewards for self, while predicting the rational actions of other players (Tonelli et al., 2017). The theory emphasizes on keep updating the security controls by considering new security threats introduced. There the cybersecurity specialists should keep considering new security threats to ICT infrastructure to update the previous set of security controls for the aim of preserving confidentiality, integrity, and availability of information. However, the theory reminds us that, when leveraging 4th industrial revolution technology for a sustainable national economy, we must also keep updating security controls against the emergence of new vulnerabilities in ICT infrastructure.

2.3 Empirical Literature Review

Cavelty, (2007) noted that computer and network vulnerabilities are therefore to be expected, and these lead to information infrastructures with in-built instabilities and critical points of failure. Moreover, many researchers agree that infrastructure is its own worst enemy because of its complexity. Systems begin to blend into one another due to the increasing use of ICTs and increasing functional demands and it is useless to try to maintain a separation of systems, each with an internally demarcated mode of responsibility.

Thus, ICT officers particularly in the public sector should not relax. They have to keep in their mind that, industrial revolution technology goes parallel with the increase of vulnerabilities. So they have to keep monitoring security vulnerabilities in their ICT infrastructure and fix them by establishing strong security controls.

Comprehensive protection of the entire critical infrastructure against all threats and risks is impossible, not only for technical and practical reasons, but also because of costs. So the greatest vulnerabilities need to be identified; those structures that are more critical, or vital points within the infrastructure. Criteria could also focus on the relative likelihood of the threat or the relative cost of protection. But when considering actual protection measures, all of these require knowledge of the nature of the threat: it makes a difference whether one needs to protect a facility against a group of well-trained attackers or whether one wants to shield information systems from unauthorized access. There is no one-fits-all solution: protection measures have to be tailored to specific assets and specific threats (Cavelty, 2007).

The problem of ensuring the protection and resilience of critical infrastructures is such that vulnerability and technical risk analyses by reductionist methods are likely to fail to capture the heterogeneity and structural and dynamic, or operational, complexities of these systems, and new approaches are needed, capable of offering a holistic viewpoint (Kröger & Zio. 2011). New solutions (security controls) against infrastructure vulnerabilities must be implemented to protect the ICT infrastructure against newly introduced attacks. So the ICT officers or cybersecurity specialists must always keep updating security controls.

The growth of Industrial Revolution Technology for a Sustainable National Economy results in a more complex technological infrastructure with more chances for emerging security vulnerabilities, which will need effective solutions for controlling them to preserve digital information against attacks which may violate confidentiality, integrity, and availability of information.

Ottino (2004) highlighted that in virtue of this evolution, the originally complicated engineered systems become complex with hallmarks of dynamic complexity such as adaptation, self-organisation and emergent behavior, which offer opportunities for extended, improved and more reliable service but also pose vulnerabilities, mostly due to unforeseen and hidden complications added during the integration process.

3. RESEARCH METHODOLOGY

3.1 Research Design

The research was structured as a case study of the Shinyanga public sector and their efforts to avoid cyber-attacks based on confidentiality, integrity and availability (CIA) of information. In interpretative information systems research, an in-depth case study is often used, as stated by Thompson et al., (2015). Analysing a specific situation in great depth and with a focus on the particulars is what a case study involves. This research focuses on the phenomena of public sector firms taking preventative measures against cyber security incidents. This phenomenon is investigated by looking at two different public entities.

3.2 Area of the Study

The researcher decided to restrict his attention to only two public organisations operating within the public sector not only to conduct more in-depth research, but also because due to the limited amount of time to devote to this thesis. The study was done at KASHWASA and SHUWASA.

3.3 Study Population

A population is the total collection of elements about which inferences are made and refers to all possible cases which are of interest to a study (Sekaran, 2003). The target population for this study was the employees at KASHWASA and SHUWASA. However, due to the vast resources, i.e. time and money that would be required to include all employees in the study, a sample of the respondents representing all employees at KASHWASA and SHUWASA, was used during the study.

3.4 The Sample Size and Sampling Techniques

The population could be a large group of individuals and it is almost impossible to collect information from all of them since they are many. Therefore a portion of the population can be chosen as representatives for the whole population, this portion of the population is called the sample (Bell & Bryman, 2007). The study applied both Simple random sampling and Purposive sampling.

Table 3.1: Sample Size Distribution of Respondents

Type of respondents	Sample size(n)	Technique for selecting sample
ICT officers /certified experts	2	Purposive
Head of ICT units/departments	2	Purposive
Other ICT users	101	Simple random
TOTAL	105	

3.4.1 Simple Random Sampling

According to Brainly website, (2019), Simple random sample is a subset of individuals (a sample) chosen from a larger set (a population). Each individual is chosen randomly and entirely by chance, such that each individual has the same probability of being chosen at any stage during the sampling process.

The study collected data from different types of respondents who are users of ICT resources. These respondents were selected randomly, hence data collected comprised the answers from respondents of different levels in the organisations.

3.4.2 Purposive Sampling

According to Brainly website, (2019), A purposive sample is a non-probability sample that is selected based on characteristics of a population and the objective of the study. Purposive sampling is also known as judgmental, selective, or subjective sampling.

This technique used in a study because it also dealt with the respondents who are knowledgeable about ICT. The respondents under this technique were ICTOs, Heads of ICT units/departments and Certified ICT experts.

According to Tongco, (2007), The purposive sampling technique is a type of non-probability sampling that is most effective when one needs to study a certain cultural domain with knowledgeable experts within. The inherent bias of the method contributes to its efficiency, and the method stays robust even when tested against random probability sampling. Choosing the purposive sample is fundamental to the quality of data gathered; thus, reliability and competence of the informant must be ensured.

3.5 Data Collection

The study included primary and secondary data collection methods focusing on quantitative data. The techniques of primary collection of data included questionnaires. While secondary data were collected from internal or external data sources of information. In short, secondary data refers to data collected by other researchers.

According to Axinn & Pearce (2006), Systematic consideration of mixed method data collection strategies reveals two key themes. The first is that mixing multiple methods affords opportunities to use the strength of some methods. Because all methods have strengths and weaknesses, combinations of multiple methods that achieve this counterbalancing aim are particularly valuable. The second theme is that mixing multiple methods is a valuable strategy for producing comprehensive empirical records about a topic.

3.6 Types and Sources of Data

The sources of data may be classified into primary sources and secondary sources. This study considered both primary and secondary data as presented below.

3.6.1 Primary Data

The primary data are those which are collected afresh and for the first time, and thus happen to be original (Kothari, 2004). They are firsthand information collected through observation, direct communication with respondents, mailing or through personal interviews. In most cases in research; observation, questionnaire and interview are common research tools which are used to

collect primary data. Regarding this study, the primary data were collected through a questionnaire and Penetration Testing.

3.6.2 Secondary Data

Secondary data are the data obtained from literature sources or data collected by other people for other purposes. Secondary data provide second-hand information and include both raw data and published ones. This implies data that are already available, and they are obtained from literature sources or data collected by other people for some other purposes which may be either published or unpublished. Therefore; secondary data provide the so called second-hand information.
According to Bryman & Bell (2015), the study would gather previously done research, industry surveys, and a proper framework to obtain additional understanding about the research that has already been conducted within the selected topic. Moreover, Flick (2018), added that, triangulation is used when one wants to validate information using at least two sources to produce better theoretical content. This is done since depending on a single source alone might lead to acquiring information that is skewed in some way.

3.7 Experience During Data Collection

The completion of the study was achieved by passing through crossover and straight thru ways. Sometimes the researcher went through unexpected situations which caused some difficulties in achieving goals. During data collection, the researcher found some of the respondents are not aware of the basics of cybersecurity issues, hence it was difficult for them to understand some questions that appeared in the questionnaire. Therefore, the research had the task of explaining the meaning of the questions in detail so the respondents to understand the questions.

Practical penetration testing was a technique which went well and led a researcher to collect data which are very relevant to the study. The research managed to find out the vulnerabilities existing in the public organisation network, and successfully exploit them to gain unauthorised access to the systems.

Online data collection using Google forms simplified to great extent the work of collecting data. The questionnaire was placed on Google form, and shared with respondents for them to provide their responses. The research managed to collect data in time, without the need of meeting with some respondents. Moreover, on Google there is a feature for automatically creating pie charts and bar graphs based on questionnaire responses, this helped the researcher in the task of analysing data.

4. FINDINGS

The results of data analysis of ICT infrastructure vulnerabilities based on confidentiality, integrity, and availability of information showed the presence of security weaknesses which can be exploited, and result in the gaining of unauthorised access to public organisation ICT infrastructure. Some of the vulnerabilities observed according to research findings were the nonexistence of firewall devices, enabling Remote Desktop Access on the server, installing remote access third-party software on the server, and using an old version of windows.

Table 4.1: Existence of Firewall device in the public organisation

A firewall in place	Freq.	Percent	Cum.
Strong Disagree	1	0.93	0.93
Disagree	27	25.23	26.17
Neutral	10	9.35	35.51
Agree	24	22.43	57.94
Strong Agree	45	42.06	100.00
Total	107	100.00	

Table 4.2: Remote Desktop Connection is enabled on the server

RDC is enabled on server	Freq.	Percent	Cum.
Strong Disagree	11	10.28	10.28
Disagree	10	9.35	19.63
Neutral	15	14.02	33.64
Agree	53	49.53	83.18
Strong Agree	18	16.82	100.00
Total	107	100.00	

Table 4.3: Installed remote access third-party software on the server

Remote access software installed	Freq.	Percent	Cum.
Strong Disagree	19	17.76	17.76
Disagree	19	17.76	35.51
Neutral	32	29.91	65.42
Agree	28	26.17	91.59
Strong Agree	9	8.41	100.00
Total	107	100.00	

Table 4.4: Using old versions of the Windows Operating System

PCs are running win 11	Freq.	Percent	Cum.
Strong Disagree	8	7.48	7.48
Disagree	57	53.27	60.75
Neutral	16	14.95	75.70
Agree	11	10.28	85.98
Strong Agree	15	14.02	100.00
Total	107	100.00	

On other hand, the results of a Practical Penetration Testing, showed the existence of infrastructure security vulnerabilities such as TCP open ports, improper naming of servers, the nonexistence of paper shredder, users' unawareness about cybersecurity etc.

Table 4.5: Penetration testing results summary

Security Model Principle tested	Vulnerabilities observed	Successfully tested attacks	Tools used to exploit vulnerabilities
Confidentiality	Improper Server naming Users' unawareness of cybersecurity Users being allowed to move with laptops outside the organisation's compound No shredding machines	Social engineering Gaining unauthorised access to laptops Cracking encrypted files	Bootsuite live CD John the ripper
Integrity	Open TCP ports	Payload Attack	Armitage (running on Kali Linux)
Availability	Open TCP port 445 Open TCP port 3389	DOS attack	Metasploit (running on Kali Linux)

5. RESULTS AND DISCUSSION

The findings indicated the existence of vulnerabilities in ICT infrastructure which can be exploited, and result in successful access gaining to the organisation's network. Various kinds of attacks like DOS, Payload, MITM can be applied to exploit the observed vulnerabilities to gain access to the organisation network. The vulnerabilities observed need to be fixed by establishing strong security controls against them.

The review of previous studies relating to vulnerability assessment highlighted that, the first step in conducting a vulnerability assessment is to identify the information assets of the facility as well as the entry points via which those information assets may be compromised (Lindgren & Jansson, 2013). The 4^{th} industrial revolution technology goes parallel with the increase of digital cybercrimes (attacks) in ICT infrastructure. So the ICT experts are alerted on taking actions for fixing all the vulnerabilities to stay free from cyber-attacks.

In this study the penetration testing was done to assess the network's vulnerabilities as it has been highlighted by the researcher in the above paragraph. The penetration testing results shown in table 3.4 helped the researcher to recommend network's security controls against cyber-attacks.

6. CONCLUSION

It has been observed that it is so important to consider confidentiality, integrity and availability of information when establishing security controls of ICT infrastructure for a public sector organisation. Failure to do that it may result in the existence of vulnerabilities which can be

exploited by cybercriminals to gain unauthorised access to the systems, change information, and make information unavailable.

Failure to incorporate all three principles of the CIA triad security model in establishing security controls will result in the presence of vulnerabilities based on a principle whose security controls have not been implemented.

Therefore, when thinking about Leveraging the 4th Industrial Revolution Technologies for a Sustainable National Economy, also security of ICT infrastructure should be given priority to preserve confidentiality, integrity, and availability of information as shown in the study.

7. RECOMMENDATION

The study results indicate the presence of vulnerabilities based on ICT infrastructure. Strong security controls must be established as preventive measures against violation of confidentiality, integrity and availability of public sector information. Therefore, the recommendations below should be considered: -

i. National Cybersecurity Standards should be set, and public organisations should be made aware of it. All the organisations must adhere to standards without failure. By doing that, it'll be possible to maintain a low or zero level of security threats index, since the vulnerabilities will be reduced hence minimal possibility of successfully cyber-attacks in public sector.
ii. Closing open ports which are not in use. This includes the ports of Operating System and Network devices such as Layer 3 Switches. Hackers normally use the open ports as vulnerability for gaining unauthorised access to the system. For example, during penetration testing conducted by the researcher, the open TCP ports were exploited by using Armitage tool and it resulted to successfully payload attack.
iii. Computer firewalls and Antivirus should always be up and running on computers. During penetration testing conducted, it was found that firewalls were off on some computers, and antivirus were not installed. Hence it was possible to gain unauthorised access to those computers, since they were vulnerable to DOS and Payload attacks.
iv. Penetration testing should be conducted time to time to find out the vulnerabilities, and fix them. The pen testers can be outsourced if there is no an expert who can to penetration testing in the organisation. The reposts for the testing should be in place for reference.
v. Proper configuration for WiFi devices should be considered. It is recommended to bind MAC addresses of employee's computers/ phones to Wi-Fi routers, so that no any other devices can be connected to Wi-Fi routers if its MAC address is not bound. This will restrict the visitors from connecting to WiFi device without consulting ICT unit. However, the range for accessing WiFi device should not go beyond organisation compound. Also, admin default login credentials for a WiFi device should be changed.
vi. To avoid using old Operation Systems which have been phased out by Microsoft, such as Ms. Windows 7. Most of these OS are vulnerable, since security updates are no more released from Microsoft. However, no more technical support provided for them from Microsoft. All computers should be updated to current OS. For example, currently the latest OS is Ms. Windows 11. Therefore, public organisations' computers should run Ms. Windows 11 for security purpose.
vii. It is advised to do daily data backup on external data center server, and the backups should be tested time to time to be sure that the can work when restored.

viii. Shredding machines for destroying papers should be used instead of destroying papers manually. This is necessary to avoid Dumpster Diving foot-printing technique.

ix. Server name should not include the word “Server”, to make it not easily being recognised when hacker is scanning the network.

8. REFERENCES

Axinn, W.G. and Pearce, L.D. (2006) *Mixed method data collection strategies*: Cambridge University Press

Bell, E. and Bryman, A. (2007) 'The ethics of management research: an exploratory content analysis', *British journal of management*.

Bell, E., Harley, B. and Bryman, A. (2015) *Business research methods*: Oxford university press.

Brainly (2019) Difference between random sample and purposive sample. Available at: https://brainly.in/question/11280286 (Accessed: 7th Oct 2022)

Cavelty, M.D., 2007. Critical information infrastructure: vulnerabilities, threats and responses. In Disarmament Forum (Vol. 3, pp. 15-22). UNIDIR.

Cordella, A. and Paletti, A. (2018) 'ICTs and value creation in public sector: Manufacturing logic vs service logic', *Information Polity*

Flick, U. (2018) *Triangulation in data collection.* The SAGE handbook of qualitative data collection.

Global Economy (2022) Tanzania: Security threats index. Available at: https://www.theglobaleconomy.com/Tanzania/security_threats_index (Accessed: 15th Sept 2022)

Khando Khando, Shang Gao, Sirajul M. Islam, Ali Salman (2021) Enhancing employees' information security awareness in private and public organisations: *A systematic literature review*

Kothari, C.R (2004) Research Methodology: Methods & Techniques. New Delhi: *New Age International (P) Limited Publishers*

Kröger, W. (2008) Critical infrastructures at risk: a need for a new conceptual approach and extended analytical tools. *Reliab Eng Syst Saf*

Lindgren, I. and Jansson, G., 2013. Electronic services in the public sector: A conceptual framework. *Government Information Quarterly*.

Ottino, J.M., 2004. Engineering complex systems. *Nature*

Sekaran, U. (2003) Research Methods for Business: A Skill Building Approach, John.

SK Media, EA [@ngurumo]. "SIRI IMEVUJA!" Twitter, 22 July 2022, https://twitter.com/ngurumo/status/1550554962316464128

Thompson, N., Ravindran, R. and Nicosia, S. (2015) Government data does not mean data governance: Lessons learned from a public sector application audit. *Government information quarterly*.

Tonelli, A.O., de Souza Bermejo, P.H., Aparecida dos Santos, P., Zuppo, L. and Zambalde, A.L., (2017) It governance in the public sector: a conceptual model. *Information Systems Frontiers*.

Tongco, M.D.C. (2007) Purposive sampling as a tool for informant selection. *Ethnobotany Research and applications*.

Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018) Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *IEEE access*.