International Journal of Information Science 2023, 13(1): 1-9
DOI: 10.5923/j.ijis.20231301.01

Assessments of Cyber Security Awareness in Higher Learning Institutions: A Case of State University of Zanzibar

Zedi A. Khamis[1], Edwin M. Kwesigabo[2,*]

[1]State University of Zanzibar, Tanzania
[2]Institute of Finance Management, Tanzania

Abstract Cyber security threats are increasing in complexity and frequency. It is crucial for higher learning institutions to prioritize cyber security awareness among students, faculty, and staff. This study has investigated Security Awareness in Higher Learning Institutions. The study employed a descriptive approach with quantitative research designation. The data were gathered from 86 samples size of employees at State University of Zanzibar (hereafter SUZA) as calculated by the Yamane formula from a total population. Data from the questionnaire were analyzed using SPSS v.26. The results from the analysis revealed that SUZA has complicated regulations and does not have sufficient manpower to raise Cyber security awareness. Also, tools for conducting risk and vulnerability assessments and preventing attacks do not meet the demands at SUZA. The findings also indicated that SUZA has challenges in the adoption of advanced technologies in Cyber security awareness and employees have minimal knowledge on measures to secure themselves from Cyber security. Correspondingly, the study findings unveiled that, SUZA has lack ICT infrastructure to protect data and devices which make organizations at risk of Cyber attacks. Moreover, the findings unveiled that, SUZA has a Cyber security policy but most employees do not know the policy. However, study findings revealed that SUZA does not perform Cyber security audits and it does not keep records of information misuse of prior intrusion challenges. This study recommends the need to make employees knowledgeable and aware of Cyber security using security awareness training. Regular trainings will enhance compliance with Cyber security policies. However, organizations need to buy the tools that are used to detect and prevent the attacks. The tools include Firewalls, Intrusion Detection and Prevention Systems, Endpoint Security Solutions, Security Information and Event Management, Antivirus and Anti-Malware Software, Data Loss Prevention, Security Awareness Training Platforms, and Encryption Solutions. Moreover, there is a need to carry out a study on the changes and dynamic nature of cybercrime in higher learning institutions.

Keywords Cyber Security, Cyber Security Awareness

1. Introduction

With the ever-growing advancements in technology, Cyber security is becoming a critical concern in today's digital age, with an ever-increasing reliance on technology and the internet. Cyber-criminals are getting increasingly sophisticated in the ways they exploit technology, making it difficult to eliminate risks. Cyber-attacks can be on technological infrastructure, in the form of malware and viruses, or on human personnel, in the form of social engineering or cyberbullying (Aldawood & Skinner, 2018). Recently, some of the fastest-growing corporate crime threats have steered away from exploiting systems or vulnerabilities in information security and instead they have focused on humans, a target considered to be the weakest link in every enterprise. In modern information technology, the world of information security has developed as a vital subject, with the human factor constituting the majority of security breaches. According to a study on Cyber security by the hacking of employees, the security of information is dependent on three primary foundations: people, processes, and technology. Researchers and experts found that even in situations where different organizations have polished procedures and sophisticated technology, the weakest link still lies in the human personnel in the process (Aldawood & Skinner, 2018).

Moreover, a number of hackers and organized cybercrime groups have grown exponentially. These cybercriminals have been adopting new methods to carry out cybercrime. The primary motivation for hacking is the financial gain obtained by stealing sensitive information and holding it for

* Corresponding author:
edwin.kwesigabo@ifm.ac.tz (Edwin M. Kwesigabo)
Received: Oct. 11, 2023; Accepted: Oct. 25, 2023; Published: Nov. 13, 2023
Published online at http://journal.sapub.org/ijis

ransom. Hackers can also earn money by selling secret data to competitors on the dark web, which makes cyberspace unsafe and poses considerable risks to organizations and their customers. Thus, Cyber security breaches have become a serious threat to global security and the economy. They target critical infrastructure and they have a considerable financial impact on business performance, and resulting in a significant loss of intellectual property (Alharbi & Tassaddiq, 2021).

Cyber security is essentially the method of maintaining cyberspace security against threats that are known and unknown. According to ITU (2016), Cyber safety is the collective implementation of policies, safety measures, plans, administrative threats tactics, commitments, training, essential procedures, and assurance and expertise that can be used to guard the data system, organization, and associated resources.

Therefore, Cyber security is now seen as a significant aspect of people and families, organizations, governments, academic Institutions, and our company. Protecting kids and family members from internet fraud is crucial for families and parents. Concerning financial safety, securing our financial data that can influence our private economic status is essential. The Internet is very essential and useful to higher learning Institutions as it used in preparing generation professional and leaders. So it is essential for higher learning institutions to prioritize cyber security awareness within the context of higher learning institutions that reflect the broader challenges and opportunities in higher education in the digital era (CISCO Report, 2015). Higher learning institutions as the main Internet consumers need to know how to safeguard themselves against online fraud and identity theft as a main prime target for cyber attacks due to the wealth of sensitive data they handle such as students records, research findings and financial information. Appropriate online behavior and system security learning result in reduced vulnerabilities and a safer online environment.

However, academic institutions employees need to understand the risk of working in academic institutions; employees can become targets (Alharbi & Tassaddiq, 2021). One of the weaknesses in academic institutions' infrastructure is the employees, who can access, change, and edit information as part of their job duties. Information system mitigation techniques and security measures are insufficient if users are unaware of the risks and those individuals or groups targeting them. Thus, organizations should conduct training and awareness sessions for employees, who should apply security policies and security training at work (Alharbi & Tassaddiq, 2021) since the most severe data breaches are caused by employees.

Cyber security is critical to organizations because they need to secure their information systems and data in cyberspace to ensure uninterrupted provision of quality products and services efficiently to their customers (Kumar, 2011). Academic institutions depend on computer networks and technologies to provide their students with university news, activities, emails, courses, academic year calendar, academic staff, student marks, and other personal information stored on their computer systems. Therefore, these systems need to be protected against several threats. It could be used by an adversary not only to affect the organization's assets by stealing their sensitive information (Al-Janabi & Al-Shourbaji, 2016). A security breach in an academic institution affects not only students but also other academic institutions' employees (Al Zaidy, 2020) and also affects the organization's financial side. However, academic institutions should take measures to protect their sensitive data and networks from ever-increasing cyber-attacks because hackers are using increasingly sophisticated approaches (Shen, 2014). Studies confirm that most employees lack awareness of cyber security in academic institutions, which may put data at risk (Qiao et al., 2020; Bada & Nurse, 2019; Gerber et al., 2018). As the techniques that attackers use to trick employees change, the importance of employee awareness increases. Hence Higher learning institutions are responsible to train their students and their staff about the importance of cyber security. Effective cyber security awareness program can mitigate risks, protect sensitive data and ensure the institutions smooth functioning in the face of evolving cyber threats. Therefore, this study seeks to explore the Cyber security awareness status of Higher learning nstitutions at Zanzibar Higher Learning Institutions.

2. Literature Review

2.1. Empirical Literature Review

Al-Janabi and Al-Shourbaji (2016) analyze the information of security awareness among academic staff, researchers, undergraduate students, and employees within educational environments in the Middle East in an attempt to understand the level of awareness of information security, the associated risks, and the overall impact on the institutions. The results reveal that the participants do not have the requisite knowledge and understanding of the importance of information security principles and their practical application in their day-to-day work. This situation can however be corrected through comprehensive awareness and training programs as well as adopting all the necessary safety measures at all levels of the institution to ensure that the students, academic staff, and employees are trustworthy and technology savvy, and keep their data safe. Without such training programs and awareness, there will be negative consequences on IT systems and their application usage, as well as on users' security now and in the future. From the weaknesses identified in this survey, some essential recommendations are put forward to remedy the situation.

Also, Koohang et al., (2019) build an awareness-centered information security policy (ISP) compliance model, asserting that awareness is the key to ISP compliance and that awareness depends upon several variables that influence successful ISP compliance. The authors built a model with

seven constructs, i.e., leadership, trusting beliefs, information security issues awareness (ISIA), ISP awareness, understanding resource vulnerability, self-efficacy (SE), and intention to comply. Seven hypotheses were stated. A sample of 285 non-management employees was used from various organizations in the USA. The authors used path modeling to analyze the data. The findings indicated that IS awareness depends on effective organizational leadership and elevated employees' trusting beliefs.

Moreover, Aldawood and Skinner, (2019) highlight pitfalls and ongoing issues that organizations encounter in the process of developing human knowledge to protect from social engineering attacks. A detailed literature review is provided to support these arguments with an analysis of contemporary approaches. The findings show that despite state-of-the-art Cyber security preparations and trained personnel, hackers are still successful in their malicious acts of stealing sensitive information that is crucial to organizations. The factors influencing users' proficiency in threat detection and mitigation have been identified as business environmental, social, political, constitutional, organizational, economic, and personal. Challenges concerning both traditional and modern tools have been analyzed to suggest the need for profiling at-risk employees (including new hires) and developing training programs at each level of the hierarchy to ensure that the hackers do not succeed.

However, Al Zaidy, (2020) examines information confidentiality and Cyber security in academic institutions. It targeted employees' training after recruitment and the ongoing training employees get during their employment at the academic institution. In this research, there are three variables: action insecurity (AI), action security (AS), and employee awareness (EA). Information security is the ultimate goal of the organization and its highest priority. The participants completed an online survey to determine employees' secure and insecure actions. The survey collected information about the everyday activities of employees in their workplaces. The study's research questions sought to determine 1) if there is a significant difference in the number of AS the employee performs before and after the training, 2) if there is a significant difference in the number of AI the employee performs before and after the training, and 3) if there is a significant difference in EA before and after the training. The study results showed no significant change in employee awareness or secure/insecure actions after the training; however, more AS and less AI were performed by the participants in terms of raw data. The study showed that academic institutions need to hire employees with a good understanding of information security, ensure that there is a plan regarding information security, and ensure that the employee knows and understands what is confidential, what is public, and how to conduct everyday activities in the scope of information security. The researcher recommends conducting similar research that targets employees' behavior and knowledge in information security for different industries.

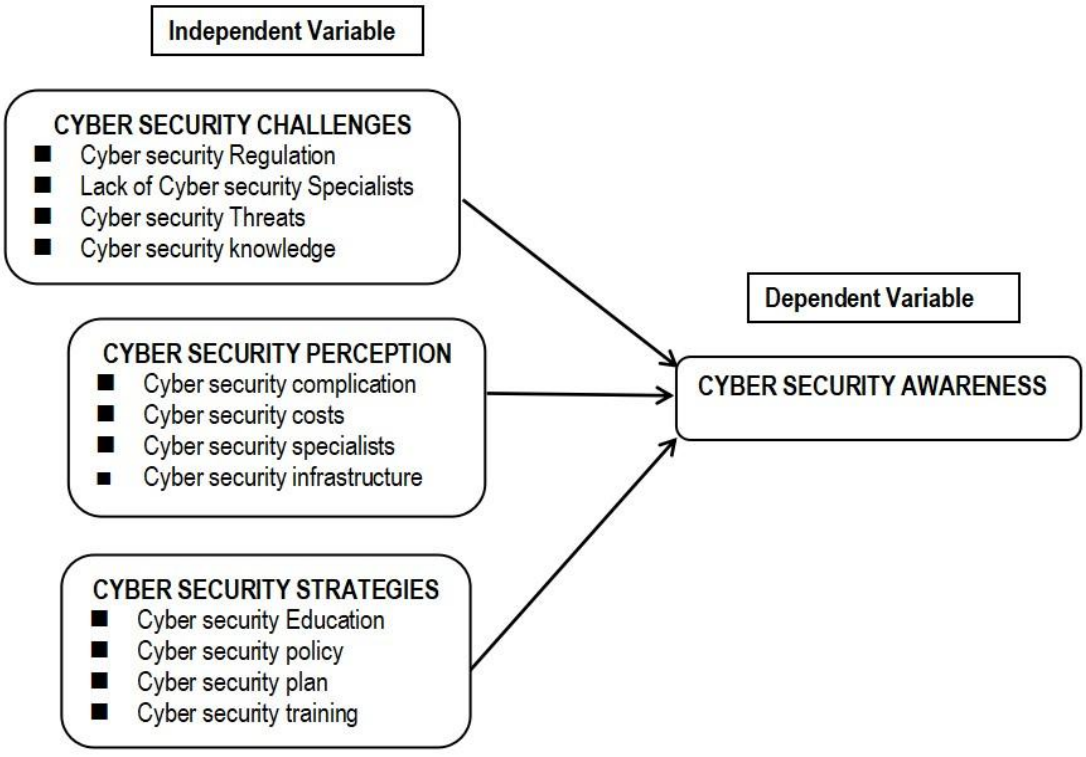

Figure 2.1. Conceptual Framework

Zwilling et al., (2020) focus on the relationships between Cyber security awareness, knowledge, and behavior with protection tools among individuals in general and across four countries: Israel, Slovenia, Poland, and Turkey in particular. Results show that internet users possess adequate Cyber threat awareness but apply only minimal protective measures usually relatively common and simple ones. The study findings also show that higher Cyber knowledge is connected to the level of Cyber awareness, beyond the differences in respondent country or gender. In addition, awareness is also connected to protection tools, but not to information they were willing to disclose. Lastly, findings exhibit differences between the explored countries that affect the interaction between awareness, knowledge, and behaviors. Results, implications, and recommendations for effective-based Cyber security training programs are presented and discussed.

2.2. Conceptual Framework

The study employed The Protection Motivation Theory and General Deterrence Theory. The major parts of the theories compose user perception of Cyber security awareness, challenges, and strategies. These parts construct the base on which the conceptual model is presented.

3. Methodology

This section presents the research design, sampling design, data collection and data analysis. A descriptive research design was used in this study. This study used a quantitative approach. As for this study, a simple random sampling technique was adopted to select a sample size. Therefore, this study adopted the Yamane's (1967) formula for sample size estimation.

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

Where;

n = Sample size, N = the population size (625), e = is the random error (95%). By Using the above formula, a sample size of 86 was obtained. In this study Primary data was collected using a questionnaire. After the data collection completed, the researcher analyzed data obtained from questionnaires using descriptive statistics with the help of the Statistical Package for Social Sciences (SPSS). Descriptive statistics, such as frequencies, percentages, mean, and standard deviation, was primarily used to summarize the data.

3.1. Validity and Reliability

The concepts of reliability and validity are core issues in determining the quality of a study. For a study to provide sufficiently sound, consistent, and relevant evidence, the information provided must be both reliable and valid (Joppe, 2000). Reliability requires the use of standardized information collection instruments and survey procedures that are designed to enhance consistency. Validity is the extent to which the survey information is relevant to the conclusion being drawn and is sufficiently accurate and complete to support the conclusion.

Validity determines whether the research truly measures that which it was intended to measure or how truthful the research results are (Joppe, 2000). To measure the validity of the instruments, the Kaiser Meyer Olkin, (KMO) method was used. The study also applied the Cronbach's Alpha technique. The technique was used for testing the reliability of the data in order to measure internal consistency.

The findings of this study revealed different coefficients (Cronbach's Alpha) of the variables as Table 3.1 indicates.

Table 3.1. Reliability Statistics: Source Field Data (2022)

Reliability Statistics		
Variable	Cronbach's Alpha	N of Items
Cyber Security Challenges	.714	7
Cyber Security Perception	.527	9
Cyber Security Strategies	.797	8
Overall Total	**.768**	**24**

Cronbach alpha coefficient test was employed to measure the internal consistency of the instruments used and the coefficient alpha of these variables was reported. According to Diedenhofen and Musch (2016), when Cronbach's alpha is greater than 0.9 (>0.9) it means that the internal consistency reliability is excellent. When it is greater than 0.8 (>0.8) the reliability is good; while greater than 0.7 is acceptable and greater than 0.6 is still acceptable. When it is 0.5 to 0.58 is poor and when it is less than 0.5, internal consistency is unacceptable. As shown in Table 3.1 above, the Cronbach alpha test indicates that the reliability of data instruments was Acceptable since the Cronbach alpha for each variable was over 0.768.

Table 3.2. KMO and Bartlett's Test: Source Field Data (2022)

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.653
Bartlett's Test of Sphericity	Approx. Chi-Square	1111.292
	df	276
	Sig.	.000

The KMO and Bartlett test was used to test validity. From the above KMO and Bartlett's Test analysis the calculated value if the test is 0.0 to 0.45 the internal adequacy is an explanatory factor is unacceptable. When it is 0.50 to 0.59 is poor; 0.60 to 0.79 is acceptable; when 0.8 to 0.89 is good and 0.9 to 0.99 is excellent. The result of the test indicated that KMO had a value of .653 which is acceptable. On the other hand, the Bartlett test in this study yielded a p-value = 0.00 which signifies that the variables are correlated highly enough to provide a reasonable basis for factor analysis as suggested by (Arbuckle, 2012) that the value for the Bartlett test should be a significance value of less than .05 as describe above in KMO and Bartlett test table 3.2.

4. Results

4.1. Descriptive Statistics

Based on the mean values, the five-point scale ranges are as follows: mean scores of less than 1.5 represents No Extent; mean scores of 1.5 but less than 2.5 represents Little Extent, mean scores of 2.5 but less than 3.5 represents Moderate Extent; mean scores of 3.5 but less than 4.5 represents Large Extent; mean scores of 4.5 to 5 represent Very Large Extent. The respondents of this study received 86 questionnaires, this is used for assessment. Using tables, major results from the research were presented. The following were specific objectives:

i. To identify Cyber Security challenges faced by the State University of Zanzibar.
ii. To examine how Cyber security is perceived by employees of State University Zanzibar.
iii. To find out the Cyber security strategies at the State University of Zanzibar.

Table 4.1. Descriptive Statistics

		Mean	Std. Deviation
Cyber security Challenges	SUZA has complicated regulations in creating Cyber security awareness among their employees.	2.77	1.299
	SUZA has enough manpower to raise Cyber security awareness.	3.17	1.416
	Employee readiness acts as a challenge to the SUZA in creating Cyber security awareness among their employees.	3.02	1.292
	Available tools to conduct risk and vulnerability assessments and prevent attacks	3.20	1.336
	Continuously adoption of advanced technologies poses a challenge to the SUZA in Cyber security awareness among their employees.	2.53	1.361
	Do you consider yourself knowledgeable about Cyber security?	3.30	1.364
	Employees make sure that their programs and systems are up-to-date regularly.	3.50	1.453
	Composite Mean	**3.0185**	
Cyber security Perception	Employees feel online safety principles are complicated.	3.26	1.303
	Employees feel adhering to online safety principles leads to a secure organization.	3.37	1.247
	SUZA has enough budget to effectively manage daily Cyber security operations and asset.	2.78	1.474
	SUZA has enough Cyber security professionals certified under internationally recognized certification programs in Cyber security.	2.71	1.502
	Employees are aware of the fake offers offered on the internet.	2.64	1.430
	Employee practice safe browsing and always	2.73	1.231
	The assets have genuinely licensed copies of the software for secure access, use, and distribution of data.	3.00	1.320
	There is secure access for users of ICT infrastructure to protect data and device.	2.43	1.538
	Employees prefer to surf and download safe websites.	3.50	1.344
	Composite Mean	**2.9355**	
Cyber security Strategies	SUZA provides education concerning Cyber security to all employees regularly.	1.93	1.254
	SUZA has established Cyber security policies.	2.48	1.124
	Employees know very well the password policy.	2.87	1.263
	Employees are aware of the requirements and importance of using a strong password.	2.97	1.324
	SUZA has established a Cyber security plan.	3.19	1.000
	SUZA carries out a Cyber risk assessment on its critical assets.	2.69	1.340
	Does SUZA regularly perform Cyber security audits and keep records of information misuse of prior intrusion challenge?	2.53	1.290
	Considering Cyber security awareness, do all members of the IT department authorized to make significant judgments related to Cyber security concerns?	2.83	1.528
	Composite Mean	**2.6862**	

From the statistical table above the result of this study indicates that the moderate extent majority of the respondents indicated that SUZA has complicated regulations in creating Cyber security awareness among their employees (Mean = 2.77, SD = 1.299). Also, these make it difficult for organizations to keep up with Cyber security technology. Study findings unveiled that, to a moderate extent SUZA has not had enough people to raise Cyber security awareness (Mean = 3.17, SD = 1.416). This implies that SUZA has a low number of an expert to raise Cyber security awareness. The majority of the respondents stated that, employee readiness act as a challenge to the SUZA in creating Cyber security awareness among their employees (Mean = 3.02, SD = 1.292). This implies that employees are not interested in Cyber security compared to other fields. However, the majority of the respondents, that have a moderate extent indicate that SUZA has limited available tools to conduct risk and vulnerability assessments and prevent attacks (Mean = 3.20, SD = 1.336). Therefore, to the moderate extent, the majority of the respondents indicated that continuous adoption of advanced technologies poses a challenge to the SUZA in Cyber security awareness among their employees (Mean = 2.53, SD = 1.361). Also, to the moderate extent, majority of the respondents indicated that the employee is not aware of Cyber security, (Mean = 3.30, SD = 1.364) and that the employee considers himself knowledgeable about Cyber security. However, to the moderate extent, majority of respondents indicate that employees make sure that their programs and systems are up to date regularly (Mean = 3.50, SD = 1.453). This implies that the employee has limited knowledge of the program and systems.

From Statistical Table above, to a moderate extent, the majority of the respondents asserted that employees feel online safety principles as complicated (Mean = 3.26, SD = 1.303). In online security safety, the findings indicate that to a moderate extent, employees feel that adhering to online safety principles leads to a secure organization (Mean = 3.37, SD = 1.247). Also, to the moderate extent, majority of the respondents indicated that SUZA does not have enough budget to effectively manage daily Cyber security operations and assets (Mean = 2.78, SD = 1.474). However, to the moderate extent, majority of the respondents indicated that SUZA has enough Cyber security professionals certified under internationally recognized certification programs in Cyber security (Mean = 2.71, SD = 1.502). Also, the study findings indicate that to the moderate extent, the majority of employees are aware of the fake offers offered on the internet (Mean = 2.64, SD = 1.430). When using the safety browser, the research findings indicate that to the moderate extent, the majority of employees practice safe browsing always (Mean = 2.73, SD = 1.231). However, the findings justify that to the moderate extent, the majority of employees have genuinely licensed copies of the software for secure access, use, and distribution of data (Mean = 3.00, SD = 1.320). Moreover, the study found that to a little extent, majority of the respondents asserted that there is secure access for users of ICT infrastructure to protect data and devices (Mean = 2.43, SD = 1.538). Also, to the moderate extent, the majority of the respondents indicate that employees prefer to surf and download on safe websites (Mean = 3.50, SD = 1.344). This implies that moderate employees use insecure websites to surf and download.

From the statistical table above, to a little extent, the majority of the respondents indicate that SUZA provides education concerning Cyber security to all employees regularly (Mean = 1.93, SD = 1.254). This shows that Cyber security education is still low for employees. However, in Cyber security policies, to a little extent, the majority of the respondents indicate that SUZA has established Cyber security policies (Mean = 2.48, SD = 1.124). This implies that SUZA has a Cyber security policy but most employees do not know the policy. Also, to the moderate extent, the majority of the employees know very well the password policy (Mean = 2.87, SD = 1.263). In this study, to the moderate extent, the majority of employees are aware of the requirement and importance of using a strong password (Mean = 2.97, SD = 1.324). Moreover, to the moderate extent, majority of the respondents indicated that SUZA has established a Cyber security plan (Mean = 3.19, SD = 1.000). Findings unveiled that, to a moderate extent SUZA carries out a Cyber risk assessment on its critical assets (Mean = 2.69, SD = 1.340). However, the moderate extent majority of the respondents indicated that SUZA regularly performs Cyber security audits and keeps records of information misuse of prior intrusion challenges (Mean = 2.53, SD = 1.290). Also, the research findings indicate to the moderate extent the majority of the respondents assert that all members of the IT department were authorized to make significant judgments related to Cyber security concerns (Mean = 2.83, SD = 1.528).

4.2. Discussion of Findings

Regarding Cyber security challenges, the results of this study indicated that SUZA has complicated regulations in creating Cyber security awareness among their employees. Findings unveiled that, to a moderate extent, majority of the respondents indicate that SUZA has no sufficient manpower to raise Cyber security awareness through employee readiness act as a challenge to SUZA in creating Cyber security awareness among their employees. These findings agree with Shaaban (2020) that one of the difficult challenges of Cyber security is to raise awareness among users. Adoption of Cyber security measures needs more focus and better practices need to be applied to increase its effectiveness. Organizations need to ensure the implementation of Cyber security in their operations at all aspects of their organizations and monitor that all stakeholders are aware and follow the Cyber security measures. There is a need to understand the Cyber security practices, challenges, and solutions for the effective implementation of Cyber security

measures (Alotaibi, 2019). Therefore, if SUZA does not manage security effectively, the effect on an organization could be very significant. The findings showed that to the moderate extent, SUZA has limited tools to conduct risk and vulnerability assessments and to prevent attacks. Study findings portray that SUZA has challenges in the adoption of advanced technologies in Cyber security awareness. Nevertheless, study findings indicate that employees have minimal knowledge of measures to secure themselves from Cyber security. These findings agree with those of Shaaban (2020), and Al-Janabi and Al-Shourbaji (2016) that the participants do not have the requisite knowledge and understanding of the importance of information security principles and their practical application in their day-to-day work. Hence, SUZA can correct it through comprehensive trainings to make sure that awareness is also connected to protection tools, such as to be able to buy tools, enhancing awareness and training programs as well as taking all the necessary safety measures at all levels of the institution to ensure that employees are honest, technology understanding and able to keep their data safe.

In Cyber security Perception the results of this study revealed that SUZA employees feel that online safety principles are complicated. They also commented that adhering to online safety principles lead to a secure organization. Nevertheless, the study found that to a little extent majority of the respondents indicate that SUZA lacks ICT infrastructure to protect data and devices which make organizations at risk of Cyber attacks. Moreover, employees use insecure websites to surf and download. The findings agree with the work of Mang'ehe (2020), the study that shows that users considered themselves safe to a very low extent while online. Cyber security depends on people. It is people's intentional and unintentional actions that cause adverse consequences that security wants to prevent. Technologies meant to provide security ultimately depend on the effective implementation and operation of these technologies by people. Also, these findings are in line with Keplain, (2020) who indicated that to keep the organization safe and secure, create a security system, increase your employee skill set, invest in your IT infrastructure and carry out a Cyber risk assessment regularly. Thence, SUZA should provide regular Cyber security education training to all employees.

In Cyber Security Strategies, the results of this study show that SUZA does not provide education concerning Cyber security to employees also SUZA has a Cyber security policy but most employees do not know the policy. Results depicted that SUZA does not conduct a Cyber risk assessment on its critical assets. Also, SUZA does not perform Cyber security audits and keep records of information misuse of prior intrusion challenges. However, the study found that the majority of the respondents disagree that all members of the IT department are authorized to make significant judgments related to Cyber security concerns. These findings agree with Kundy (2019) who indicated that Cyber threats were exacerbated in higher education institutions due to insufficient network security policies and practices involving management, insufficient information technology structures, and poor Cyber security understanding of ICT infrastructure, properties, and exposures. Moreover, these findings are in line with Koohang et al., (2019) that information security awareness depends on effective organizational leadership and elevated employees' trusting beliefs. Also, compliance with Cyber security policies, security awareness and training should be provided regularly to influence employees.. Therefore, this calls for additional efforts from the government and institutions to reshape this situation.

5. Conclusions and Recommendations

This study assessed the Cyber security awareness in Higher learning institutions in Zanzibar. More specifically, this study tried to identify Cyber security challenges faced by the State University of Zanzibar, to examine how Cyber security is perceived by employees of State University Zanzibar and to find out the Cyber security strategies of the State University of Zanzibar.

From the findings, the research has produced many outcomes to assess the Cyber security in SUZA in this study, including employees who have minimal knowledge of measures to secure themselves from attacks. To address this issue, employers need to make employees knowledgeable and aware of Cyber security using specific awareness programs that should be developed by educational and academic institutions because a security threat cannot be avoided or reported if it is not recognized. Also, SUZA has limited tools to conduct risk and vulnerability assessments and prevent attacks. To address this issue, organizations need to buy the tools that are used to detect and prevent attacks. There are specifics of successful Cyber security awareness training programs and their impact on organizations.

KnowBe4 at St. Luke's University Health Network is a system that runs a Cyber security training platform. This program focuses on phishing simulations and Cyber security awareness. The impact of this program is to reduce Phishing Susceptibility, Improved Employee Awareness, and Enhanced Data Security (Mansfield-Devine, 2018).

However, the SANS Security Awareness Program at Emory University partnered with the SANS Institute to implement a comprehensive security awareness program, including phishing simulations, online training, and resources. The impact of this in the organization to reduction in the click rate on simulated phishing emails and Increased Incident Reporting, employees need more proactive in reporting security incidents, which improves the incident response process (Labuschagne & Eloff, 2014).

The success of these programs highlights the importance of investing in cybersecurity awareness initiatives and can serve as inspiration for SUZA management to implement similar efforts to protect their organization from cyber threats.

Nevertheless, this study concludes that Cyber security strategies, for example Cyber security policy, passwords policy, organization device policy, and audit plan by involved management and the finding showed that SUZA has not had enough budget to effectively manage daily Cyber security operations and assets. SUZA also does not have enough Cyber security professionals certified by an international organization. Therefore, education on the institution's policies for employees is needed, so the institution will be required to provide policy education for its employees. It can be concluded that it is possible to keep SUZA secured, despite some challenges than frustrate the Cyber security awareness programs and implementation strategies.

Based on the findings from the study, the following recommendations are therefore made:

i. According to the study's conclusions, the HLI management needs to implement the proposed Cyber security awareness training to build a security culture in the organization and enhance employee awareness of Cyber security while reducing security risks. More importantly, this is meant to bring about compliance with the Cyber security policies.
ii. Also, there is a need to invest in cybersecurity tools and technology, since much of HLI lacks the necessary tools to protect against Cyber attacks. Even so, it is important to invest in Cyber security tools to change the perception of Cyber attacks in detection and prevention. Some essential tools and technology include Firewalls, Intrusion Detection and Prevention Systems, Endpoint Security Solutions, Security Information and Event Management, Antivirus and Anti-Malware Software, Data Loss Prevention, Security Awareness Training Platforms, and Encryption Solutions.
iii. Despite active efforts to raise Cyber security, the field is contentious to the experience. There is a shortage of individuals interested in the career which is a significant concern. A policy on Cyber security awareness should be advocated. To close this gap, HLIs must initiate training in Cyber security strategies.

Therefore, further studies should focus on the impact of training on employee actions and Cyber security awareness in Higher Learning Institutions in Zanzibar Higher Learning Institutions. Also, other studies should be conducted in other sectors for comparison and generalization of findings.

REFERENCES

[1] Al Zaidy, A., 2020. Impact of Training on Employee Actions and Information Security Awareness in Academic Institutions (Doctoral dissertation, Northcentral University).

[2] Aldawood, H. and Skinner, G., 2018, December. Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)* (pp. 62-68). IEEE.

[3] Aldawood, H. and Skinner, G., 2019, May. Challenges of implementing training and awareness programs targeting cyber security social engineering. In 2019 cybersecurity and cyber forensics conference (ccc) (pp. 111-117). IEEE.

[4] Aldawood, H. and Skinner, G., 2019. Reviewing cyber security social engineering training and awareness programs-Pitfalls and ongoing issues. Future Internet, 11(3), p.73.

[5] Alharbi, T. and Tassaddiq, A., 2021. Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2), p.23.

[6] Al-Janabi, S. and Al-Shourbaji, I., 2016. A study of cyber security awareness in educational environment in the middle east. Journal of Information & Knowledge Management, 15(01), p.1650007.

[7] Arbuckle, J.L., 2012. IBM SPSS Amos 21. Chicago, IL: Amos Development Corporation.

[8] Bada, M. and Nurse, J.R., 2019. Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). Information & Computer Security.

[9] CISCO Report, (2015) what-is-cybersecurity.aspx. Retrieved from http://www.itgovernance.co.uk:http://www.itgovernance.co.uk/whatiscybersecurity.asx.

[10] Diedenhofen, B. and Musch, J., 2016. cocron: A Web Interface and R Package for the Statistical Comparison of Cronbach's Alpha Coefficients. *International Journal of Internet Science, 11(1)*.

[11] Gerber, N., Gerber, P., Drews, H., Kirchner, E., Schlegel, N., Schmidt, T. and Scholz, L., 2018, December. Foxit: enhancing mobile users' privacy behavior by increasing knowledge andawareness. In Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust (pp. 53-63).

[12] Joppe, G., 2000. Testing reliability and validity of research instruments. J*ournal of American Academy of Business Cambridge*, 4(1/2), pp.49-54.

[13] Koohang, A., Anderson, J., Nord, J.H. and Paliszkiewicz, J., 2020. Building an awareness-centered information security policy compliance model. Industrial Management & Data Systems.

[14] Kumar, D.A. and Balakrishnan, V., 2011. A study on ISO 9001 quality management system certifications–reasons behind the failure of ISO certified organizations. Global Journal of Management and Business Research, 11(9), pp.43-50.

[15] Kundy, E. 2019. Assessment of the cyber security threats in higher learning Institutions in Tanzania, A case of University of Arusha and Tumaini University Makumira. Master's Thesis. Institute of Accountancy Arusha.

[16] Labuschagne, W. A., & Eloff, M. (2014). The effectiveness of online gaming as part of a security awareness program. In 13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece (p. 125).

[17] Mansfield-Devine, S. (2018). The ever-changing face of

phishing. Computer Fraud & Security, 2018(11), 17-19.

[18] Shaaban Y. S. 2020. Assessment of Cybersecurity Awareness Among Employees in Banking Industry in Tanzania: A Case of National Microfinance Bank NMB. Magomeni Branch. Master's thesis. Institute of Accountancy Arusha.

[19] Shen, L., 2014. The NIST cybersecurity framework: Overview and potential impacts. SciTech Lawyer, 10(4), p.16.

[20] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N., 2022. Cyber security awareness, knowledge, and behavior: a comparative study. Journal of Computer Information Systems, 62(1), pp.82-97.