The Journal of Informatics, Vol. 4, Issue 1 (pages 128-149)
eISSN: 2953-254X, ISSN: 2714-1993 (Print)
Received: September, 2024, Published: October, 2024
DOI: https://doi.org/10.59645/tji.v4i1.355

****Original Research****

USERS' AWARENESS OF CYBER SECURITY PRACTICES FOR PREVENTING DATA ATTACKS IN PUBLIC ORGANISATIONS

Authors
Mishael Emanuel Abduel
Faculty of Informatics
Institute of Accountancy Arusha
ORCiD: https://orcid.org/0009-0004-0326-6610

Abstract

This study assessed users' awareness of cyber security practices for preventing data attacks. The study employed a descriptive research design and quantitative research approach. A random sampling technique was used to select a sample of 65 respondents. Data were collected through structured questionnaires. Descriptive statistics such as mean and standard deviation were used to analyse data. The validity and reliability of data collection tools were ensured. Findings revealed that the user's awareness of cyber security practices on prevention of data attacks was high in the selected case for study, which remains anonymous. The study recommends that due to the rapid changing of technology, the organisation should prevent risks from various sources, including internet-borne attacks, such as spyware or malware, user-generated weaknesses, such as easily guessed passwords or misplaced information, inherent system or software flaws and vulnerabilities and subvert system or software features.

Keywords: User's Awareness of Cyber Security, Data Attacks, Theory of Planned Behaviour

1. INTRODUCTION

Cyber security awareness is vital in both public and private organisations as it ensures that the organisation's data is safe from attacks from both internal and external bad actors (Fransiska and Tobing, 2023). Organisations are striving to implement cyber security awareness because the threat scenery of data attacks is rapidly changing, and the potential impact of such attacks is uncertain (Tufail et al., 2021). Global information society emerged with no borders, and this has brought new opportunities for every country in the world whereby technology performs an ever-increasing essential role in developing the social and economic aspects of life (Adomako et al., 2018). News of data breaches and online frauds has become a matter of regular occurrence, which serves as a constant reminder and a strong urge for cyber security awareness that organisations need a robust strategy for fraud prevention and cyber security. In many organisations, cyber security practices and awareness have been known to be effective in preventing data attacks. This is because one of the most challenging issues that come with advancements in technology is securing systems from cyber-attacks (Li & Liu, 2021).

Worldwide, there have been various studies on cyber security practices for the prevention of data attacks in public organisations. For instance, Tvaronavičienė et al. (2020) indicated that in the United Kingdom, more than 1,000 cyber-attacks in the previous year (which increased by 14% from 2017). Among these, 95% of respondents were using antivirus, firewall, and malware protection. On the other hand, about 38% of respondents said they had not experienced any cyber-attacks at all, compared to 30% the year before that. The types of attacks most

commonly faced by the respondent organisations included phishing (95%), malware (86%), and ransomware (54%). Other attacks, such as targeted attacks from insiders or malicious cybercriminals, were faced by only 3% of respondents. In Indonesia, Fransiska and Tobing (2023) revealed that public organisations have invested in cyber security, including awareness of cyber security among team members in order to prevent data attacks.

Moreover, the government has also prioritised raising awareness among public users on how they can detect and report data attacks. This helps the organisation understand fraud risk and apply best practices. This can also enable the organisation to manage risk and improve the security of critical data.

Similarly, Tufail et al. (2021) realised that in developing countries like Cameroon, although employees in organisations have a good knowledge of information technology, their awareness of cyber security remains limited; thus, they are vulnerable to data attacks. The study also found that most organisations have no policies regarding cyber security practices; thus, they are susceptible to data attacks. On the other hand, a survey by Kabanda (2018) in Zimbabwe realised that despite the efforts invested in cyber security infrastructures in public organisations, data attack incidents have increasingly been reported.

In Uganda, Adomako et al. (2018) indicated that there is no global consensus on how to regulate and respond to cyber-attacks; therefore, African countries like Uganda tend to adopt policies and laws intended for developed nations that possess much higher response capabilities. Even countries with cybercrime laws remain vulnerable to awareness challenges as efforts to date have been mostly ineffective in preventing or prosecuting attacks.

According to Assenga (2020), the Tanzania Communications Regulatory Authority (TCRA) is responsible for the supervision, monitoring, and licensing of stakeholders in the telecommunications industry, as well as for enforcing cyber-related activities. Therefore, cyber security falls under the telecommunications sector. The constitution of the United Republic of Tanzania protects individuals' and organisations' privacy and personal communication, information, or interference/interception of one's communication. Affected individuals can seek relief from the relevant authorities against anyone who unlawfully gains access to, destroys, alters, conceals, and uses personal information or information stored on another

person's device without their consent or the due process of the law (Temu, 2021).

In many public organisations, data attack incidents have been reported. These attacks cause reputational damage, theft, and financial losses, as reported by Koloseni, Lee, and Gan (2019). This problem has made public organisations adopt various cyber security practices to prevent data attacks through cyber security practices because the threat scenery of data attacks is rapidly changing, and the potential impact of such attacks is uncertain.

Among the current cyber security practices adopted by public organisations include making a backup of the organisation's data, ensuring that there is a backup of the confidential files, keeping track of who accesses the system, Wi-Fi protection, personal accounts for employees, separate username and passwords, having manual cyber security policies as well as setting online safety guidelines (Tufail et al., 2021). Despite the cyber security practices done by public organisations, the problem of data attack incidents still exists. Therefore, there was a need to assess the user's awareness of cyber security practices as part of mechanisms for the prevention of data attacks.

2. OBJECTIVE OF THE STUDY

This study assessed users' awareness of cyber security practices for preventing data attacks in public organisations. One case study was selected in the Arusha Region. However, its identity remains anonymous for security reasons.

3. LITERATURE REVIEW

This section covers the review of literature based on the theory employed in the study as well as empirical evidence from other studies related to cyber security awareness.

3.1 Theoretical Review on the Theory of Planned Behaviour

The theory of planned behaviour framework guided the study. The theory was initially proposed by Icek Ajzen and is found to be suitable because it has been used in investigating individuals' ethical behaviour and decisions with respect to the adoption of and compliance with computer security measures (Conner, 2020). The Theory of Planned Behaviour assumes that individuals act rationally, according to their attitudes, subjective norms, and perceived behavioural control. These factors are not necessarily actively or consciously considered

during decision-making but form the backdrop for the decision-making process (Ajzen, 2020).

According to the theory of planned behaviour, behaviours are influenced by intentions, which are determined by three factors: attitudes, subjective norms, and perceived behavioural control (Miller, 2017). It is also possible for external factors to directly force or prevent behaviours, regardless of the intention, depending on the degree to which the individual actually controls behaviour and the degree to which perceived behavioural control is an accurate measure of actual behavioural control. In other words, people may not articulate a particular attitude, but it may nonetheless influence their decision-making (Bosnjak, Ajzen & Schmidt, 2020).

In relation to this study, the theory of planned behaviour demonstrates how the attitude, subjective norms, and perceived behavioural control of employees in public institutions affect the way they mitigate cyber-attacks. These behaviours, among others, can be shaped through various awareness-raising strategies. This is to say, when the level of awareness of cyber security (independent variable) is high, they can be in a position to mitigate data attacks (dependent variable). Therefore, through this theory, the researcher was able to achieve the objective of the study.

3.2 Empirical Literature Review Users' Awareness of Cyber Security Practices

A study by Nasir, Arshah, Hamid, and Fahmy (2019) found in the literature for assessing cyber security awareness also investigating which methodologies were applied, who was the target audience, and whether the coverage of previous assessments of cyber security awareness was comprehensive or not. During their literature search, the author found studies that matched the search criteria, and the information about the authors, publication year, assessment method used, target audiences, coverage of assessment, and assessment goals were extracted from each article. The authors found that younger audiences were not explored as a target of evaluation as in-depth as would be required. This is seen as particularly concerning due to the amount of exposure and damage that this target could incur in case of security incidents.

Moreover, Li and Liu (2021), in a comprehensive review study of cyber-attacks and cyber security, reported that at present, most of the economic, commercial, cultural, social, and

governmental activities and interactions of countries at all levels, including individuals, non-governmental organisations and government and governmental institutions, are carried out in cyberspace. Recently, many private companies and government organisations around the world have been facing the problem of cyber-attacks and the danger of wireless communication technologies partly due to a lack of awareness. Today's world is highly dependent on electronic technology, and protecting this data from cyber-attacks is a challenging issue. The purpose of cyber-attacks is to harm companies financially. In some other cases, cyber-attacks can have military or political purposes. Some of these damages are PC viruses, knowledge breaks, data distribution services (DDS), and other assault vectors. To this end, various organisations use various solutions to prevent damage caused by cyber-attacks. Cyber security follows real-time information on the latest IT data.

Srinivas, Das, and Kumar (2019) examined government regulations in cybersecurity, highlighting the complexity of new technologies and the uncertainty in their adoption. Their study suggests that cybersecurity awareness plays a crucial role in shaping attitudes and intentions toward learning and using the latest technologies. However, these attitudes may be ill-formed or evolve only after initial attempts to use the technology. Consequently, the actual implementation of cybersecurity awareness measures may not directly follow from these initial attitudes, emphasising the need for comprehensive awareness programmes that bridge the gap between intention and action in cybersecurity practices.

Furthermore, Szczepaniuk et al. (2020), in their study on information security assessment in public administration, indicated that cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Implementing safe cyber security best awareness practices is essential for individuals as well as organisations of all sizes. Using strong passwords, updating your software, thinking before you click on suspicious links, and turning on multi-factor authentication are the basics of what we call "cyber hygiene" and will drastically improve your online safety. These cyber security basics apply to both individuals and organisations. For government and private entities, developing and implementing tailored cyber security plans, awareness programmes, and processes is critical to protecting and maintaining business operations. As information technology becomes increasingly integrated with all aspects of our society, there is an increased risk for

wide-scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend.

Moreover, Sarker et al. (2020), in their review of cyber security data science, found that there are many reasons why people make data attacks, including financial gain, espionage, activism, and sabotage. In some cases, cyber-attacks may be politically motivated to cause damage to their opponents. Data attacks can happen in various methods. For instance, a hacker can use phishing methods to trick a user into clicking a malicious link or entering their login credentials into a fake website. Alternatively, a hacker may damage the vulnerability in the software by accessing other devices to steal sensitive information. In this context, organisations are advised to invest in cybersecurity awareness practices.

Similarly, Hasan et al. (2021), when evaluating the cyber security readiness of organisations and its influence on performance, indicated that the top ten system vulnerabilities account for approximately 85% of data breaches; some have been around for as long as several years but continue to be exploited. Roughly 80% of successful attacks originate with external threat agents, but the majority also involve either deliberate or accidental actions by "insiders," i.e., members or employees of the victimised organisation; a typical example is an attack that starts with "phishing" to trick an insider into revealing information or downloading malware, giving the attacker access to the system. Cyber security ensures the protection of information systems, such as hardware, software, and related infrastructure, data on these systems, and the services provided by these systems, which can be done by illegal access by adversaries (intruders or attackers). Sometimes, intentional harm can be caused by an operator of the system. Therefore, either deliberate or accidental harm can result in failing to obey the security procedures.

On the other hand, Hart et al. (2020), in their study on games for cyber security awareness and education, revealed that one of the significant challenges facing many organisations is the lack of awareness among the users. This has put many organisations at risk. It was further noted that information and communications technology ICT is ubiquitous and continually evolving. It is increasingly integral to modern society. ICT devices and components form a highly interdependent system of networks, infrastructure, and resident data known as cyberspace. Cyber security is essential in protecting cyberspace from attacks by criminals and other adversaries. The risks associated with any such attack depend on three factors:

threats that are attacking, vulnerabilities and weaknesses they are attacking, and impact on how the attack affects the victims.

A study conducted in Tanzania by Mtakati and Sengati (2021) on the cyber security posture of higher learning institutions indicated that despite implementing minimal countermeasures, the study discovered that Higher Learning Institutions are vulnerable to cyber-attacks. Higher Learning Institutions must be vigilant by addressing identified weaknesses, providing cyber security training to all staff, and continuously monitoring information systems. The study recommends an increase in cyber security awareness and exploration of the factors affecting cyber security preparedness in higher learning institutions.

Another study was conducted by Kundy and Lyimo (2019) on cyber security threats in higher learning institutions in Tanzania. It was revealed that poor implementation and adherence to cyber security strategy and standards by involved management, weak information infrastructure systems, and employees' poor cyber security awareness relative to ICT infrastructures, assets, and exposures involved influence cyber threats in higher learning Institutions. Moreover, study findings revealed cyber threat countermeasures implemented at the University of Arusha and Tumaini University Makumira include continuous monitoring of inbound network traffic load on firewalls and system resources (CPUs), segmentation of internal and external networks for critical, cyber risk assessment on critical assets and constantly scanning and patching for software vulnerabilities.

Woldemichael (2019) further argues that cybercrime is estimated to have cost the global economy just under USD 1 trillion in 2020, indicating an increase of more than 50% since 2018. With the average cyber insurance claim rising from USD 145,000 in 2019 to USD 359,000 in 2020, there is a growing necessity for better cyber information sources, standardised databases, mandatory reporting, and public awareness. A preliminary search resulting in 5219 cyber peer-reviewed studies showed that the application of systematic methodology resulted in 79 unique datasets. We posit that the lack of available data on cyber risk poses a severe problem for stakeholders seeking to tackle this issue. In particular, we identify a lacuna in open databases that undermines collective endeavours to manage this set of risks better. The resulting data evaluation and categorisation will support cyber security researchers and the insurance industry in their efforts to comprehend, metricise and manage cyber risks.

In the ongoing digital era, cyber-security threats have become considerable enough to have reached mainstream attention, with major cyber-attack cases reaching the headlines of multiple media outlets. One of the significant targets of cyber-attacks in recent years has been critical infrastructures from all sides of the industry. For example, one of the most infamous cyber-attacks in recent years was a campaign against industrial control systems, known by the codename Dragonfly. According to technical reports, attackers exploited a variety of techniques, including attaching malware to third-party programmes, e-mails, and websites to gain access to numerous computer systems. By doing so, the attackers were able to mount sabotage operations that could have disrupted energy supplies across several. Often, the success of such attacks was determined by user unawareness and lack of formal training of staff. In a 2015 study, 31% of security breaches in industrial firms during that year were attributed to human errors. In another study, it was found that the root cause of 80% of data breaches can be attributed to stolen data, often obtained through social engineering attacks such as e-mail phishing. All these studies and reports show that one of the critical factors in the success of many cyber-attacks is user awareness and training, as reported by Woldemichael (2019).

Fu et al. (2020) realised that one of the main advantages of integrating training as a measure to increase cyber security awareness in daily activities is that it aids in retaining information for longer than traditional training and that it allows this information to be transferred into other activities. Other forms of training analysed by the authors include classroom training, experiment-based training, interactive games, material sharing, user knowledge, and intelligent measurement. The authors conclude that interactive methods have shown a greater degree of success in effectively training personnel and students. Embedded solutions, in particular, have been shown to allow trainees to retain information for the longest. One criticism of the research conducted by the authors is that the data utilised come from different training sessions that included different materials, modules, and objectives. Standardisation of all these attributes would be necessary to extrapolate objective conclusions about the advantages and disadvantages of each solution.

Woldemichael (2019) examined the emerging cybersecurity threats in organisations and found that cyber-security is a preventive preparation of protecting sensitive information, information systems, computers, servers, critical infrastructure, mobile devices, and

computer networks from unauthorised access or hackers. Nowadays, digital technology plays the most significant role in the growth, effectiveness, and efficiency of the organisation. However, new technologies like mobile technologies (5G), IoT, and cloud computing are Coming with new information security threats. Employees' awareness is low, and they are still using the old software, they did not update the software (operating system), they use a permanent password, they are still using weak and default passwords (Wife name or her phone number) information security literacy and behaviour end users or IT staff. They do not have an awareness of proactive cyber-attack prevention policies and procedures due to the failure to take short- and long-term training on the most serious cyber-attacks, such as ransomware, social engineering, malware, DDoS, and phishing. The findings demonstrate that cyber security preparations and trained employees are very low; hackers are becoming more sophisticated.

A study conducted by Bada, Sasse, and Nurse (2019) on cyber security awareness campaigns in Mexico found that cyber security awareness is necessary for both organisations' employers and employees. Awareness should focus on changing behaviour. The study further noted that changing behaviour requires more than providing information about risks of cyber security ineffectiveness. Through cyber security awareness campaigns, the organisation's information safety will be guaranteed. Fu, Kohno, Lopresti, Mynatt, Nahrstedt, Patel, Richardson, and Zorn (2020), in their work on safety, security, and privacy threats posed by accelerating trends in the Internet of Things revealed that cyber security in organisations should be given priority so as to reduce information insecurity. In this context, the organisation's information will be safe.

A survey conducted by Tirumala, Valluri, and Babu (2019) on cyber security awareness concerns, practices, and conceptual measures indicated that current technological advances have required the discovery of numerous aspects of cyber security in both local and international organisations and institutions. The introduction of sophisticated communication devices has forced both government and private organisations to create awareness of cyber threats and cyber security for the safety of their information. The study further reported that due to the importance of cyber security on the safety of organisations, some developed countries like New Zealand have mandated to implement cyber security procedures in various sectors.

Nasir, Arshah, Hamid, and Fahmy (2019) analysed the dimensions of the information security culture concept. The study indicated that the primary role of any organisation is to ensure the safety of its information, both related to operations and those related to employees. It was further agreed that technological advancement, especially on information technological devices in organisations, should go hand in hand with innovative and creative strategies to safeguard their information in public organisations. In light of the risk and potential consequences of cyber events, CISA strengthens the security and resilience of cyberspace, a vital homeland security mission. CISA offers a range of cybersecurity services and resources focused on operational resilience, cybersecurity practices, organisational management of external dependencies, and other critical elements of a robust and resilient cyber framework. CISA helps individuals and organisations to be aware, communicate current cyber trends and attacks, manage cyber risks, strengthen defences, and implement preventive measures. Every mitigated risk or prevented attack enhances the nation's cybersecurity.

A current study by Zwilling, Klien, Lesjak, Wiechetek, Cetin, and Basim (2022) on cyber security awareness, knowledge, and behaviour indicated that in many organisations, information safety is a challenge to increasing data usage and internet consumption. However, in countries like Israel, Slovenia, Poland, and Turkey, cyber threat awareness among organisations is high. This assures the safety of information within an organisation. On the other hand, individuals that use internet possess adequate cyber threat awareness but apply only minimal protective measures, usually relatively common and simple ones.

A study on evaluating the cyber security readiness of organisations and its influence on performance was conducted by Hasan, Ali, Kurnia, and Thurasamy (2021). It was found that the acceleration of cyber-attacks in recent years has negatively impacted the overall performance of organisations around the world. Organisations face the challenge of a lack of awareness of cyber security to prevent and combat cyber-attacks. The study further indicated that when information in the organisation is attacked, both financial and non-financial problems occur, thus affecting the reputation and the performance of the organisation.

In Zimbabwe, a study conducted by Kurebwa and Magumise (2020) on the effectiveness of cyber security frameworks in combating terrorism in Zimbabwe reported that cyber threats in developing countries have been underreported but have been just as severe and even more devastating. The study further noted that cyber fraud and theft are some of the significant

cyber security threats in Zimbabwe. Zimbabwe lacks awareness of this issue, and there is a lack of established legislation and other regulatory institutions for cybersecurity. Among the recommendations is that the Ministry of Justice, Legal and Parliamentary Affairs enact cyber security laws in Zimbabwe to combat cyber terrorism. This indicates that the failure to have adequate policies and regulations on cyber security in the country, both public and private organisations, puts them at risk from hackers.

A study by Reegård, Blackett, and Katta (2019) on the concept of cyber security culture found that cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Implementing safe cyber security best practices is essential for individuals as well as organisations of all sizes. Using strong passwords, updating your software, thinking before you click on suspicious links, and turning on multi-factor authentication are the basics of what we call "cyber hygiene" and will drastically improve your online safety. These cyber security basics apply to both individuals and organisations. For government and private entities, developing and implementing tailored cyber security awareness plans and processes is critical to protecting and maintaining business operations. As information technology becomes increasingly integrated with all aspects of our society, there is an increased risk for wide-scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend.

4. METHODOLOGY

A descriptive research design was used to achieve the main objective of the study. The design was used to obtain information that describes the existing phenomena by asking individuals about their perceptions, attitudes, and values. Based on the nature of the study, the researcher used a quantitative approach to address research questions for the best results. The quantitative approach helped the researcher to collect data from various respondents' settings, which were then used to compare the findings. Through a quantitative approach, the researcher was able to present data using tables.

Sampling

The targeted population included officers and IT experts from the anonymous organisation in the Arusha regional office. The total number of population of officers and IT experts was

100. A sample of 65 respondents was obtained through the Yaro Yamane Statistical formula, and a random sampling technique was employed.

Data Collection Method

Primary data were collected using closed-ended questionnaires. According to Taherdoost (2021), questionnaires are practical and cover a large number and area compared to other methods like interviews. Questionnaires are generally less expensive and do not consume much time. In this study, the questionnaire techniques enabled the researcher to reach many respondents in a short period of time. The closed-ended questionnaires were prepared in English language. The questionnaires had five options for respondents to indicate their level of agreement or disagreement as follows: 1= Strongly Disagree, 2= Disagree, 3= Undecided/Neutral, 4 = Agree, and 5= Strongly Agree.

Data Analysis

Descriptive analysis was employed in data analysis. Descriptive statistics such as mean and standard deviation were used in data analysis. Data were collected, coded, and then entered into the software (SPSS version 26.0). Interpretation of findings was done using a Five Point Likert Scale.

Quality Procedures

The validity of the instruments for data collection in this study was done through expert review. Experts in research, including the supervisor, went through the questionnaires and gave comments to ensure that the content was well understood and matched with the research questions that guided the study. To ensure the reliability of data collection instruments in this study, the researcher conducted questionnaire testing through a pilot study. Respondents for the pilot study were selected randomly. Data obtained from the pilot study were tested through SPSS to ensure internal consistency. The test yielded the Cronbach's Alpha of 0.806, and this proved that the data collection instruments were reliable, as shown in Table 1.

Table 1: Reliability Results

Objective	Items	Cronbach's Alpha
User's Awareness of Cyber Security Practices	6	.806

Source: Field Data (2023)

5. RESULTS

This study intends to assess the user's awareness of cyber security practices as part of mechanisms for the prevention of data attacks. In this regard, the study collected data through a closed-ended questionnaire from respondents, including officers and IT personnel. The data were descriptively analysed, and the results and discussions are presented below.

5.1 Findings Presentation

A total of 65 questionnaires were distributed to respondents; 60 (92.3%) were filled and returned. The researcher was successful in collecting the filled questionnaires as respondents were obtained at one point. To achieve the objective of the study, respondents were asked to respond to various statements in the questionnaire. The rating of these statements was based on a 5-point Likert Scale ranging from 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4= Agree, to 5= Strongly Agree. The mean score interpretation scale was as follows: Mean scores from 1 to 1.80 were interpreted as strongly disagree. Mean scores from 1.81 to 2.60 were interpreted as disagree. Mean scores from 2.61 to 3.40 were interpreted as Neutral/Undecided. Mean scores from 3.41 to 4.20 were interpreted as agree, and mean scores from 4.21 to 5.00 were interpreted as strongly agree. The results of the analysis are shown in Table 2.

Table 2**:** Descriptive Statistics on User's Awareness of Cyber Security Practices

User's awareness	n	Mean	St. Dev	Overall rating
I am aware of the use of strong passwords	60	4.94	.53902	Strongly Agree
I am aware of having separate accounts	60	4.04	.86110	Agree
I am aware of never sharing credentials with others	60	4.75	.62914	Strongly Agree
I am aware of the changing passwords in three months	60	3.53	.86433	Agree
I am aware of detecting any indicator of cyber attacks	60	4.16	.74936	Agree
I am aware of blocking and reporting unsafe links	60	3.80	.88477	Agree

Source: Field Data (2023)

Table 2 presents findings about the user's awareness of cyber security practices on the prevention of data attacks. It was revealed that respondents strongly agreed that users were aware of the use of strong passwords and never sharing credentials with others, with the mean score of 4.94 and 4.75. Moreover, Table 4.5 indicated that respondents agreed that users were aware of having separate accounts, changing passwords in three months, detecting any indicator of cyber-attacks, and blocking and reporting unsafe links with mean scores of 4.04, 3.53, 4.16, and 3.80, respectively. Generally, findings imply that the user's awareness of cybersecurity practices in the prevention of data attacks was high. Moreover, the findings indicate that the organisation had various initiatives to raise awareness of cyber security practices among users.

5.2 Findings Discussion

5.2.1. Awareness of Strong Passwords

This study examined respondents' awareness of strong passwords. The findings show a very high level of understanding regarding the use of strong passwords, with a mean score of 4.94, which stands for "Strongly Agree". This aligns with recent research emphasising the importance of password security in cybersecurity awareness. For instance, Kostic and Saveljic (2023) developed a gamified approach to elevate password strength awareness, highlighting the ongoing need for education in this area (Kostic & Saveljic, 2023). Similarly, Alotaibi et al. (2018) created a mobile game called "Password Protector" to educate users about creating strong and complex passwords, demonstrating the continued focus on this aspect of cybersecurity. On top of the above, Herath et al. (2022) also identified password security as a key area of concern in their systematic literature review on cybersecurity practices for social media users. The high awareness level in the current study suggests that efforts to educate users about strong passwords have been largely successful, though ongoing reinforcement may be necessary.

5.2.2. Awareness of Having Separate Accounts

The issue of awareness of having separate accounts was noted as crucial in this study. The findings indicate a good level of awareness regarding the use of separate accounts, with a mean score of 4.04, which means "Agree". This awareness is crucial in the context of modern cybersecurity practices, as supported by Chasanah and Candiwan (2020), who identified

identity theft as one of the six focus areas in their study on cybersecurity awareness among college students in Indonesia, emphasising the importance of account security. The use of separate accounts can mitigate the risk of widespread compromise if one account is breached. Additionally, Löffler et al. (2021) incorporated this concept into their virtual escape room game designed to raise cybersecurity awareness, further highlighting its significance in current cybersecurity education efforts. The relatively high awareness level in the current study confirms that users are increasingly recognising the importance of account separation, though there may still be room for improvement.

5.2.3. Awareness of Never Sharing Credentials

The study investigated the issue of sharing credentials whereby the findings show a very high level of awareness regarding the importance of not sharing credentials, with a mean score of 4.75 and an overall rating of "Strongly Agree". This aligns with current cybersecurity best practices and recent research. Concepcion and Palaoag (2024) emphasised the importance of promoting cyber hygiene among academic employees, which includes safeguarding credentials. Lubua and Pretorius (2019) insisted on the need for policy and procedure compliance, which considers the issue of sharing credentials as critical. Taherdoost (2024) proposed an Integrated Cybersecurity Awareness Training (iCAT) model that incorporates various aspects of cybersecurity, including credential protection. The high awareness level in the current study implies that users understand the critical nature of keeping credentials private, which is a positive indicator for overall cybersecurity posture.

5.2.4. Awareness of Changing Passwords Regularly

Changing passwords is a critical issue in addressing cybersecurity issues. In this study, the findings indicate a moderate level of awareness regarding the practice of changing passwords every three months, with a mean score of 3.53 which indicates "Agree". This awareness level, while positive, is lower than for other password-related practices. Recent literature has begun to question the efficacy of frequent password changes. For example, Kioskli et al. (2023) discussed the evolving nature of cybersecurity best practices in healthcare, noting that mandatory frequent password changes can sometimes lead to weaker passwords (Kioskli et al., 2023). The moderate awareness level in the current study may reflect this ongoing debate in the cybersecurity community about the optimal frequency of password changes.

5.2.5. Awareness of Detecting Indicators of Cyber Attacks

In assessing the awareness of detecting indicators of cyber-attacks, the findings of the study in this area show a good level of awareness regarding the ability to detect indicators of cyber-attacks, with a mean score of 4.16 (Agree). This confirms that awareness is crucial in any organisation's current cybersecurity landscape. The findings concur with Asiri et al. (2023), who conducted a comprehensive review of Indicators of Compromise (IoCs) in Industrial Control Systems, highlighting the importance of recognising attack indicators. Additionally, Merlino et al. (2022) developed a situational awareness tool to detect system compromise by monitoring IoCs of DDoS attacks, further emphasising the significance of this skill. The relatively high awareness level in the current study implies that users are becoming more adept at recognising potential threats, though there may still be room for improvement through continued education and training.

5.2.6. Awareness of Blocking and Reporting Unsafe Links

Unsafe links are everywhere, and creating awareness of blocking and reporting them seems to be crucial. In this regard, the findings indicate a moderate level of awareness regarding blocking and reporting unsafe links, with a mean score of 3.80 and an overall rating of "Agree". This awareness is essential in preventing phishing attacks and other link-based threats. The findings aligned with those of Chasanah and Candiwan (2020), who identified phishing as one of the key focus areas in their study on cybersecurity awareness. Furthermore, Domínguez-Dorado et al. (2023) proposed a "Wide-Scope CyberSOC" approach to enhance holistic awareness among cybersecurity teams, which includes the ability to identify and respond to unsafe links. The moderate awareness level in the current study suggests that while users have some understanding of the importance of handling unsafe links, there may be a need for more focused education and training in this area.

6. CONCLUSION AND RECOMMENDATION

6.1. Conclusion

The study reveals a generally high level of cybersecurity awareness, particularly in areas such as using strong passwords, not sharing credentials, and detecting indicators of cyber-attacks. However, there are variations in awareness levels across different aspects of cybersecurity. While respondents showed very high awareness of the importance of strong passwords and not sharing credentials, there was relatively lower awareness regarding practices like changing passwords regularly and blocking and reporting unsafe links. These findings align with recent

research in the field, highlighting both the successes of current cybersecurity education efforts and areas that may require further attention. The study confirms the dynamic nature of cybersecurity awareness, reflecting ongoing debates in the field, such as the efficacy of frequent password changes, and emphasising the need for continual adaptation of cybersecurity education strategies.

6.2. Recommendations

The study recommends that due to the rapid changing of technology, there should be efforts to prevent risks from various sources, including internet-borne attacks, such as spyware or malware, user-generated weaknesses, such as easily guessed passwords or misplaced information, inherent system or software flaws and vulnerabilities and subvert system or software features. The study further recommends that the organisation maintain its control access to data and systems to make sure that individuals can only access data and services for which they are authorised. The study further recommends that organisations should ensure that they use up-to-date software since cyber-attacks happen because the systems or software are not entirely up to date, leaving weaknesses.

REFERENCES

Adomako, K., Mohamed, N., Garba, A., & Saint, M. (2018, March). Assessing cybersecurity policy effectiveness in Africa via a cybersecurity liability index. TPRC.

Ajzen, I. (2020). The theory of planned behaviour: Frequently asked questions. Human Behavior and Emerging Technologies, 2(4), 314-324.

Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. Sensors, 21(20), 6901.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2018). Design and Evaluation of Mobile Games for Enhancing Cyber Security Awareness. *Journal of Internet Technology and Secured Transactions*.

Asenahabi, B. M. (2019). Basics of research design: A guide to selecting appropriate research design. *International Journal of Contemporary Applied Researches*, 6(5), 76-89.

Asiri, M., Saxena, N., Gjomemo, R., & Burnap, P. (2023). Understanding Indicators of Compromise against Cyber-attacks in Industrial Control Systems: A Security Perspective. ACM Transactions on Cyber-Physical Systems, 7, 1-33.

Assenga, M. G. (2020). The Effectiveness of Leadership Styles to the Performance of Tanzania Public Organization: A Case of Tanzania Communication and Regulatory Authority (TCRA) (Doctoral dissertation, Mzumbe University).

Bhardwaj, P. (2019). Types of sampling in research. *Journal of the Practice of Cardiovascular Sciences*, 5(3), 157.

Bosnjak, M., Ajzen, I., & Schmidt, P. (2020). The theory of planned behaviour: Selected recent advances and applications. *Europe's Journal of Psychology*, 16(3), 352.

Chasanah, B. R., & Candiwan, C. (2020). Analysis of College Students' Cybersecurity Awareness in Indonesia. SISFORMA.

Concepcion, J. D., & Palaoag, T. D. (2024). An Assessment of Cybersecurity Awareness among Academic Employees at Quirino State University: Promoting Cyber Hygiene. *Journal of Electrical Systems.*

Domínguez-Dorado, M., Rodríguez-Pérez, F. J., Carmona-Murillo, J., Cortés-Polo, D., & Calle-Cancho, J. (2023). Boosting Holistic Cybersecurity Awareness with Outsourced Wide-Scope CyberSOC: A Generalisation from a Spanish Public Organization Study. Information, 14, 586.

Fransiska, F. B., & Tobing, F. B. (2023). Securing Indonesia Cyber Space: Strategies for Cyber Security in the Digital Era. *Jurnal Studi Sosial dan Politik*, 7(1), 50-62.

Ghiasi, M., Dehghani, M., Niknam, T., Kavousi-Fard, A., Siano, P., & Alhelou, H. H. (2021). Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform. Ieee Access, 9, 29429-29440.

Granić, A., & Marangunić, N. (2019). Technology acceptance model in educational context: A systematic literature review. *British Journal of Educational Technology*, 50(5), 2572-2593.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. Computers & Security, 95, 101827.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organisations and its influence on performance. *Journal of Information Security and Applications*, 58, 102726.

Hasib, M. (2022). Cybersecurity leadership: powering the modern organisation (Vol. 1). Tomorrow's Strategy Today.

Herath, T. B. G., Khanna, P., Ahmed, M., & Ani, O. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal of Cybersecurity and Privacy*, 2, 1-18.

Kabanda, G. (2018). A Cybersecurity culture framework and its impact on Zimbabwean organisations. *Asian Journal of Management, Engineering & Computer Science*, 3(4), 17-34.

Kamal, S. A., Shafiq, M., & Kakria, P. (2020). Investigating acceptance of telemedicine services through an extended technology acceptance model (TAM). Technology in Society, 60, 101212.

Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. Applied Sciences.

Koloseni, D. N., Lee, C. Y., & Gan, M. L. (2019). Understanding information security behaviours of Tanzanian government employees: a health belief model perspective. *International Journal of Technology and Human Interaction* (IJTHI), 15(1), 15-32.

Kostic, M., & Saveljic, I. (2023). Gamification as a Tool for Elevating Password Strength Awareness. BISEC.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, 8(6), 898.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.

Löffler, E., Schneider, B., Zanwar, T., & Asprion, P. (2021). CySecEscape 2.0 - A Virtual Escape Room To Raise Cybersecurity Awareness. *International Journal of Serious Games*, 8, 59-70.

Loishyn, A. A., Hohoniants, S., YaTkach, M., Tyshchenko, M. H., Tarasenko, N. M., & Kyvliuk, V. S. (2021). Development of the Concept of Cybersecurity of the Organization. *TEM Journal*, 10(3), 1447.

Lubua, E. W., & Pretorius, P. D. (2019). Cyber-security policy framework and procedural compliance in public organisations. In Proceedings of the International Conference on Industrial Engineering and Operations Management (pp. 1-13).

Mellinger, C. D., & Hanson, T. A. (2020). Methodological considerations for survey research: Validity, reliability, and quantitative analysis. Linguistica Antverpiensia, New Series–Themes in Translation Studies, 19.

Merlino, J. C., Asiri, M., & Saxena, N. (2022). DDoS Cyber-Incident Detection in Smart Grids. Sustainability.

Mölder, F., Jablonski, K. P., Letcher, B., Hall, M. B., Tomkins-Tinch, C. H., Sochat, V.,... & Köster, J. (2021). Sustainable data analysis with Snakemake. F1000Research, 10.

Mtakati, B., & Sengati, F. (2021). Cyber security Posture of Higher Learning Institutions in Tanzania. *The Journal of Informatics*, 1(1).

Mueller, R. O., & Knapp, T. R. (2018). Reliability and validity. In the Reviewer's Guide to Quantitative Methods in the Social Sciences (pp. 397-401). Routledge.

Opie, C. (2019). Research approaches. Getting Started in Your Educational Research: Design, Data Production and Analysis, 137.

Paté-Cornell, M. E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis*, 38(2), 226-241.

Rafique, H., Almagrabi, A. O., Shamim, A., Anwar, F., & Bashir, A. K. (2020). Investigating the acceptance of mobile library applications with an extended technology acceptance model (TAM): C*omputers & Education*, 145, 103732.

Reegård, K., Blackett, C., & Katta, V. (2019). The concept of a cybersecurity culture. In 29th European Safety and Reliability Conference (pp. 4036-4043).

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from a machine learning perspective. *Journal of Big Data*, 7, 1-29.

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering*, 7(11), 125-128.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems*, 92, 178-188.

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security*, 90, 101709.

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, 12(3), 417-432.

Taherdoost, H. (2021). Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects. *International Journal of Academic Research in Management* (IJARM), 10(1), 10-38.

Taherdoost, H. (2024). Towards an Innovative Model for Cybersecurity Awareness Training. Information.

Temu, G. (2021). Regulation and Enforcement of Competition Law in Tanzania's Telecommunications Sector: Law, Institutional Design and Practice. Universitaet Bayreuth (Germany).

Tufail, S., Parvez, I., Batool, S., & Sarwat, A. (2021). A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. *Energies*, 14(18), 5894.

Tvaronavičienė, M., Plėta, T., Della Casa, S., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into regional development*, 2(4), 802-813.

Ustundag, A., Cevikcan, E., Ervural, B. C., & Ervural, B. (2018). Overview of cyber security in the Industry 4.0 era. Industry 4.0: *managing the digital transformation,* 267-284.

Wang, S., & Wang, H. (2019). Knowledge management for cybersecurity in business organisations: a case study. *Journal of Computer Information Systems.*

Woldemichael, H. T. (2019). Emerging Cyber Security Threats in Organization. *International Journal of Scientific Research in Network Security and Communication,* 7(6), 7-10.

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J.,... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1-25.