Tanzania Journal of Engineering and Technology 2024, **43**(1):204-215
OPEN ACCESS articles distributed under Creative Commons Attribution Licence [CC BY-ND]
Websites: https://ajol.org/tjet; https://tjet.udsm.ac.tz

ISSN 1821-536X (**print**); ISSN 2619-8789 (**electronic**)
https://doi.org/10.52339/tjet.v43i1.1022

Regular Research Manuscript

Evaluation of Cybersecurity in Remote Working Settings for Mobile Network Operators

Hillary J. Teri[1,2] and Victoria Mahabi[2†]

[1,2]Vodacom, P.O. Box 35131, Dar es Salaam, Tanzania.

[2]Mechanical and Industrial Engineering Department, College of Engineering and Technology, University of Dar es Salaam, P.O. Box 35131, Dar es Salaam, Tanzania.

[†]**Corresponding Author:** vmahabi@gmail.com

[†]ORCID: https://orcid.org/0000-0002-0719-7411

ABSTRACT

Cybersecurity has increasingly been a primary concern to people as technology advances and allows them to work remotely. This study thus evaluated the cybersecurity posture for organisations that have opted for remote working culture, whereas emerging cyber threats, practices to combat them, and appropriate guidelines for managing cyber threats were discussed. The study used a descriptive design with a quantitative approach from 118 information technology personnel working for Tanzania's three major mobile network operators (MNOs). SPSS analysed the collected data. The study revealed that predominant cyber-threats affecting MNOs in remote working include human errors, phishing attacks, malicious domains, denial of service, and ransomware. At the same time, highly applied cybersecurity controls are virtual private networks, antivirus, staff training, and two-factor authentication. The study recommends that MNOs constantly be alerted to every cyber threat; they should provide advanced cyber training and follow cybersecurity guidelines for remote working settings.

ARTICLE INFO

Submitted: **Aug. 23, 2023**

Revised: **March 26, 2024**

Accepted: **Apr, 23, 2024**

Published: **June., 2024**

Keywords: Cyber security, mobile network operators, remote working, two-factor authentication, virtual private networks, staff training, Tanzania.

INTRODUCTION

Nowadays, businesses' economies and daily operations in any country depend on technology and cyber infrastructure. It is also evident that most people do work, play, shop, socialise (Chou et al., 2022), bank, and pay taxes online via available technologies such as the Internet, and therefore, on-boarded infrastructure needs to be well secured against cyber threats (Al-Sartawi, 2020; Moturi et al., 2021). Cybersecurity, also called information technology security, describes many activities to protect end-user computers, networks, programs, and data from unauthorised access or attacks (PAC, 2013; Moturi et al., 2021; Sposato, 2021).

Remote work is not a new norm that has emerged in recent years; it started even before the Industrial Revolution when everyone worked out of their homes. Skilled blacksmiths, carpenters, leather workers and potters set up workshops at their residences and sold their goods. However, with the industrial revolution, a need for automation and the creation of factories was raised (Taifa et al., 2020; Maganga and Taifa, 2022); thus, giant

machines and large-scale productions required employees to be present in-house to complete their work (Nchalala et al., 2022; Mwasubila et al., 2022). But this working culture started to change as technology advances as the introduction of computers and the Internet allowed people to connect their homes to the World Wide Web (www) and, hence, paved the way to work from anywhere (remote working) (Medromi et al., 2014; Sposato, 2021).

Although individuals and organisations had started practising remote working (Sposato, 2021), especially those in developed countries, the uptake of this working normal throughout the world was accelerated to a more significant extent upon the outbreak of the Corona Virus Disease (COVID-19) pandemic that originated in Wuhan-China in 2019 (Ponemon Institute 2020; Di Gennaro et al., 2020). Later, the virus propagated to almost all countries and forced individuals to keep a distance from each other to avoid further contamination and transmission (Di Gennaro et al., 2020). The same trend was also observed in Tanzania as some of the high-tech organisations, including MNOs, were as well striving to control the outbreak of COVID.

From theories and past reviews, it is observed that remote workers are the number one target for hackers or cyberbullying (Ponemon Institute, 2020). This is because they operate and access sensitive organisational and individual information from an environment that is not monitored and controlled regarding cybersecurity (Ponemon Institute, 2020). Unfortunately, required cybersecurity controls cannot be enforced in central offices or locations (Ponemon Institute, 2020).

According to Baldini *et al*. (2020), cyber threats emerged way back in the 1970s when computer systems were introduced; the same gained popularity in the 1990s with the introduction of the Internet and the World Wide Web (www), whereas software and network security started to be prioritised by some of organisations and governments. In the 2000s, the number of internet users increased considerably paving the way for remote working and attributed to an increase in cyber-attack techniques such as viruses and warms, including the "I LOVE YOU" worm, which spread like wildfire in May 2000, infecting over 50 million systems worldwide during its first ten days (Baldini *et al*., 2020). Not only that, the world's digital transformation in the 2010s led to the introduction of the significant data phenomenon and artificial intelligence (AI) (Taifa *et al.*, 2020; 2021; Maganga and Taifa, 2022) that geared up the remote working culture and created new challenges for cybersecurity as cybercriminals managed to capitalise on opportunities offered by these developments and introduce cyber-attacks such as ransomware (Baldini *et al.*, 2020). It has also been observed that organisations that have let their workforce work from remote or home no longer have control over their devices and networks and hence subject their cybersecurity posture to high risks related to their systems and data (Chbib, 2021). Chbib (2021) acknowledged this by mentioning the risks these organisations are subjected to unencrypted file sharing, insecure Wi-Fi, phishing, bringing your device, human errors, malicious domains, and ransomware.

Most organisations and individuals have been considering cybersecurity practices to protect their information (Baldini et al., 2020; Malatji et al., 2020; Senarak, 2021). Data is being compromised even before the shift to remote working. But with remote working, many new loopholes have been created, forcing them to invest more in cybersecurity (Wessels et al., 2021). According to Acharya (2018), before most organisations shifted to remote working, they focused more on guiding their central office's perimeters to ensure all their systems and data were protected against cyber threats. They were doing so because 90% of their work was carried out within their organisation's environment, and

hence the deployment and usage of these controls, "a package sniffer (network protocol analyser), honeypot and wireless network tools", were appropriate (Acharya, 2018). But, with the shift to remote working, most of the mentioned cybersecurity controls started becoming ineffective as cybersecurity risks gradually shifted to remote locations. Therefore, additional techniques, tools and practices were required to overcome emerging concerns. Thus, past research have revealed that additional controls such as; virtual private network (VPN) (Durbin, 2021), portals (Jain and Pal, 2017), remote computer access service (Sheshadri, 2022), two factors authentication (2FA) (Sadri and Asaar, 2021), end-user training and regular data backups (Kechagias et al., 2022) to preserve cybersecurity posture for organisations that have opted for remote working.

Deploying cybersecurity controls is insufficient to ensure cybersecurity hygiene, especially for organisations with a remote working culture (Kertysova et al., 2018). Organisations should also be guided by certain cybersecurity frameworks or guidelines that clearly define appropriate strategies, tools, processes and procedures to enhance their cybersecurity (Kertysova et al., 2018; Morze and Smyrnova-Trybulska, 2021). According to Shuster (2021), a cybersecurity framework or guideline acts as a checklist that guides a particular organisation in dealing with all aspects of cybersecurity issues, so organisations should incorporate it to overcome noted challenges. A National Institute of Standards and Technology (NIST) guideline was reviewed. This guideline or framework has already been adopted by some organisations, such as "RiverSafe" and has assisted in enhancing their cybersecurity (Shuster, 2021). The framework is divided into five individual functions, each representing a set of activities and objectives that need to be achieved (Shuster, 2021). Together, these functions are essential for businesses to build a holistic and comprehensive cybersecurity strategy. The five pillars of the NIST framework include identifying (IT assets, business environment, governance and risk management strategy); protecting (applying appropriate tools to remediate noted vulnerabilities and risks); detecting (implementing monitoring tools and processes for detecting unforeseen cybersecurity threats); respond (tools and processes to auto-respond to security threats) and recover (processes to help organisations get back to normal after a cyber-event) (Shuster, 2021).

Furthermore, Salamzada et al. (2015) proposed a Malaysian cybersecurity framework after conducting interviews with some Malaysian experts in ICT, cyber security, and cybercrime. Based on their suggestions, a guideline was developed with six pillars required by government sectors to enhance their cybersecurity; effective governance, cybersecurity emergency readiness, protecting critical information infrastructure, technology innovation, international cooperation, and legislative and regulatory framework (Salamzada et al., 2015). Therefore, this research intends to evaluate cybersecurity in remote working settings for mobile network operators. The research was guided by the following questions: What are cyber threats targeting MNOs in remote working?, What are the applied cybersecurity controls in remote working? and What are the guidelines for enhancing cybersecurity in remote working?

METHODS AND MATERIALS

Research design

Due to the nature of this study, a descriptive design was adopted to assess the cybersecurity stance of MNOs as they opted for remote working normally. Based on the statistical data, the study has also adopted a quantitative research design to describe a particular situation or problem. The target population involved the IT

personnel of three MNOs in Tanzania, including Vodacom Tanzania Limited, Millicom (Tigo) Tanzania Limited, and Airtel Tanzania Limited. The selection of these companies was based on the market share criterion. By June 2021, the operators' subscription market shares for the three companies were as follows: Vodacom had 30.0%, Airtel (26.6%), and Tigo (24.4%) (TCRA, 2021). Therefore, since these companies are nearly at the same level in market share, so are their strategies, operations, exposure to cyber threats, and cybersecurity controls. Also, the decision to involve only the IT personnel was because they are mostly involved in planning, discovering, designing, developing, maintaining, and protecting the company's technologies and, hence, much involved in addressing cybersecurity concerns (Sposato, 2021). The proportion of IT personnel for the selected companies was 71 for Vodacom, Airtel (50) and Tigo (53). However, to ensure the true representativeness of the population, the sample size for the entire population was initially determined using Taro Yamen's formula, as cited by Taifa (2016), with a 95% confidence level (equation 1) and later, the actual sample size for each company, i.e. Vodacom, Airtel, and Tigo, was determined as shown in Table 1.

$$n = \frac{N}{1+Ne^2} \quad (1)$$

where n = the sample size, N = population of the study area, and e = acceptable error restriction. For this study, the acceptable error restriction will be 0.05.

Table 1: **Population sample**

Total sample size				**The required sample size for each group**				
Total population	**N**	**174**	a	MNO	Population (174)	Ratio	Sample	Sample Size
	e	0.05	b					
	e^2	0.0025	c	Vodacom	71	0.4080	49.78161	**50**
	$a \times d$	0.435	d	Airtel	50	0.2874	35.05747	**35**
	$1 + d$	1.435	f	Tigo	53	0.3046	37.16092	**37**
Total Sample	$\frac{a}{f}$	121.25						**122**

Data collection instrument

The main instrument that was used in the data collection from the selected respondents was a questionnaire. This questionnaire comprised closed-ended statements, while the secondary data source involved findings from previous studies. Questionnaires were opted for data collection due to the following reasons: their potential to reach out to a large number of respondents within a short time, being able to give respondents adequate time to respond to the items, offering a sense of security (confidentiality) to the respondent and lastly, it is the objective method since no bias resulting from the personal characteristics (as in an interview) (Owens, 2002).

Type of data

The study involved both primary and secondary data. In collecting primary data, the study administered questionnaires to the selected sample and collected them after they were filled. The collected data were about the first two research questions. Secondary data were collected from reviewed literature and previous studies regarding understanding the guidelines or framework for enhancing cybersecurity in remote working.

Data quality

Data quality is generally understood to be the degree to which data, including research processes such as data collection and statistical accuracy, meet users' needs (Radhakrishna et al., 2012). A researcher must ensure that the data used in the study have the qualities needed for use. In this

study, data quality was measured in two ways, i.e. the reliability test and validity.

Validity of data

Pre-testing of the questionnaire, expert suggestions, discussions, and readings from various documented reports were considered to ensure data reliability and validity. The questions for the questionnaire were also reviewed, whereby unclear questions were revised, and complex items were reworked.

Reliability of data

Data reliability is defined as internal consistency (Taifa, 2016). The instrument or questionnaire can measure what it is supposed to measure (Nchalala et al., 2022). In measuring the reliability of the study, the collected data were subjected to SPSS, and Cronbach's Alpha test was run. Collected data were then checked for reliability before being analysed, of which Cronbach's Alpha was used. The test revealed a reliability of 0.8795, which is reliable as a reliability value above 0.7 is considered statistically acceptable (Taifa, 2016).

Data analysis

After data was collected, it was cleaned and presented, starting with the demographic characteristics of respondents and ending with the objective questions. A descriptive analysis was used to address the first and second objectives, whereby questionnaire responses were keyed into SPSS for analysis, and the output was exported through frequency tables and inferential statistical tables.

RESULTS AND DISCUSSION

Demographic information and Reliability testing

During the survey, 122 questionnaires were distributed; 118 responses qualified to be used for analysis, thus making a 92% response rate. But also, the Cronbach Alpha test values for cyber-threats and cybersecurity control that yielded 0.86 and 0.873, respectively, proved the extent to which the study measurement or questionnaire remains the same. The study explored the profile of respondents involved in terms of age. This was done to ensure that all age groups had their comments on the study matter to get a diversified opinion, knowledge, and experience about cybersecurity. The result of the age profile of the respondents was as follows: 18-35 years (51), 36-45 years (42), 46-50 years (16), and above 50 years (9 respondents). This shows that the majority of respondents are young and middle-aged individuals.

The study also investigated the participants' work experience to ensure the data's quality. As per common sense, a person with high experience in IT would have gathered good knowledge and experience on IT-related issues, including cybersecurity. The profile of the participants in terms of work experience in IT was as follows: 1 month to 2 years (19 respondents), above 2 to 5 years (25), above 5 to 10 years (38), above 10 to 20 years (27) and above 20 years (8). These results imply that 63 per cent of the study participants had a work experience of above 5 years. Thus, the study sample was in an excellent position to comment on cybersecurity matters, implying that the data collected was of good quality.

Understanding the working levels of the study participants was another vital aspect of the investigation. This is because getting a combination of staff who work at different levels would enhance data quality because different work levels are associated with different roles, responsibilities, and exposure. So, the study participants' profiles for the work level were as follows: junior staff (5), supervisor (36), middle-level manager (17), senior manager (12) and directors (3). Most study participants work in junior (42%) and supervisor positions (31%). Most respondents are at low and middle working

levels due to the respective companies' organisational structure. However, the observed style supports the study's intents since low and middle-level staff are more directly involved in troubleshooting works and, thus, more likely to encounter cyber-attack cases in their daily work. So, blending these two groups delivered a diversified opinion and experience that ensured the quality of collected data.

Cyber-threats occurring during remote working at the selected MNOs

The study evaluated cyber threats that occur during remote working and their rate or chance of occurrence. This aspect was measured in terms of respondents stating whether or not the provided cyber-threat has occurred and the frequency at which it has occurred (Table 2).

Table 2: Cyber-threats targeting remote working

Cyber threat	Very frequently	Frequently	Occasionally	Rarely	Never
Ransomware attack	1%	2%	2%	9%	86%
Human errors	48%	24%	17%	9.3%	1.7%
Phishing attack	36%	31%	19.5%	7.6%	6.8%
Malicious domain	28%	30%	24%	15%	3%
Denial of service attacks	21%	24%	25%	27%	3%

Inferential statistics were also used to analyse and interpret the basic characteristics of the data with regard to cyber threats affecting MNOs during remote working (Table 3). Each response was ranked as "*most frequently = 5", "frequently = 4", "occasionally = 3", "rarely = 2", and "never = 1*". Table 3 shows that human error is a leading cybersecurity threat affecting selected MNOs followed by phishing attacks, malicious domain attacks, denial of service attacks and ransomware attacks in that order. These results resemble several past researches that also appreciated that human error is the number one threat to organisations that have opted for remote working. According to Nabe (2020), prior to massive remote working, human error was already one of the major causes of cyber threats to organisations, as employees would unknowingly or recklessly give access to the wrong people. With remote working, the risk is high as sometimes, when employees are working from home or remotely are interrupted by family members or social visitors in their work, which leads to exposure to cyber threats.

Applied cybersecurity controls for remote working at the selected MNOs

The study also investigated cybersecurity measures applied at MNOs to counter cyber breaches in remote working. Several measures were identified and analysed based on their applicability by the selected MNOs during staff remote working. The results of the analysis are shown in Table 4. Inferential statistics were also used to interpret the basic characteristics of the data concerning the applied cyber-attacks at the selected MNOs. Each response was rated as "highly applied =5", "moderately applied = 4", "slightly applied = 3", "not applied = 2", and "never = 1". The summary of the study results is shown in Table 5.

Table 2: **Analysis of the basic characteristics of the cyber threats**

	Statistics				
Variable	Human Error	Ransomware attack	Denial of Service Attacks	Malicious Domain	Phishing Attacks

N	Valid	118	118	118	118	118
	Missing	0	0	0	0	0
Mean		3.1440	1.8960	2.4160	2.8080	3.0080
Median		3.0000	1.0000	2.0000	3.0000	3.0000
Mode		4.00	1.00	1.00	3.00	3.00[a]
Std. Deviation		1.21273	1.04450	1.24242	1.22274	1.25400
Skewness		-.401	.023	.475	-.136	-.065
Std. Error of Skewness		.217	.217	.217	.217	.217
Kurtosis		-.863	-.639	-.699	-1.008	-1.008
Std. Error of Kurtosis		.430	.430	.430	.430	.430
Minimum		1	1	1	1	1
Maximum		5	5	5	5	5
Sum		393.00	287.00	302.00	351.00	376.00

[a]. Multiple modes exist. The smallest value is shown

Table 3: **Applied cybersecurity controls for remote working**

Cybersecurity control	Highly applied	Moderately applied	Slightly applied	Not applied	Never
Training employee's basic cybersecurity principles	38%	20%	30%	6%	6%
Antivirus and regular backups	53%	28%	19%	0%	0%
Packet sniffer (Network Protocol Analyser)	12.7%	24%	43%	9.3%	11%
Virtual Private Network (VPN)	45%	39%	9%	6.3%	0.7%
Two-factor authentication (2FA)	33%	31%	25%	7.6%	3.4%
Remote computer access Service	27%	32%	23%	9.5%	8.5%

Table 5 indicates that VPN is the most applied cybersecurity control by organisations that have opted for a remote working culture followed by antivirus and regular backups, staff training, 2FA, remote computer access service and network protocol analyser. These results are contrary to cyber-threat results that indicate that human error is a leading threat affecting MNOs in remote working, so the most applicable control would be staff or user training. They also conflict with several past research studies revealing that the emphasis on VPN use is insufficient without proper staff or user training programs. According to Beyer and Brummel (2015), properly trained end-users develop skills required to confidently and safely navigate cyberspace at work and home and eliminate several other threats while working remotely. Therefore, the results indicate a mismatch between "the cause" and "the control", which could signify inefficiency in cybersecurity management by these organisations. The observed gap suggests a need for a guideline to ensure effective cyber control based on the intensity of the attacks.

Guideline for enhancing cybersecurity in remote working

The study reviewed and analysed two global frameworks being applied by companies and states, NIST and Malaysian cybersecurity frameworks. The analysis aimed to scrutinise the strengths and weaknesses of each framework while trying to match with MNOs' settings to blend and establish guidelines that fit the MNOs. The analysis of the NIST framework showed that it is mostly applicable to companies of different sizes and industries that have opted for remote working. On the other hand, the Malaysian cybersecurity framework is good, except it is based on specific public sectors and governments. So, it does not suit private

companies. After learning the modality of the two frameworks and considering MNOs' settings, the NIST framework was the most appropriate. The framework was adapted to make it more compatible with the MNOs, thus resulting in new guidelines for remote work. These newly developed guidelines were presented to respondents for evaluation. The validation results showed that 89% of the respondents accepted the new guidelines, while 11% were not completely content. The proposed guidelines are in Table 6.

Table 4: **Basic characteristics of the data with regards to applied cyber-attacks**

Statistics							
		Two Factor Authentication	Remote Computer Access Service	Virtual Private Network	Packet Sniffer	Employee Training	Antivirus & Backup
N	Valid	118	118	118	118	118	118
	Missing	0	0	0	0	0	0
Mean		2.8800	2.4880	3.4480	2.3680	2.9360	3.2160
Median		3.0000	3.0000	4.0000	2.0000	3.0000	3.0000
Mode		3.00	3.00	5.00	1.00	3.00[a]	3.00
Std. Deviation		1.20215	1.21560	1.50513	1.25426	1.33649	1.20204
Skewness		-.303	.302	-.569	.467	-.108	-.483
Std. Error of Skewness		.217	.217	.217	.217	.217	.217
Kurtosis		-.826	-.815	-1.129	-.838	-1.152	-.516
Std. Error of Kurtosis		.430	.430	.430	.430	.430	.430
Minimum		1.00	1.00	1.00	1.00	1.00	1.00
Maximum		5.00	5.00	5.00	5.00	5.00	5.00
Sum		360.00	311.00	431.00	296.00	367.00	402.00

[a]. Multiple modes exist. The smallest value is shown

Respondents were also asked to provide their analysis of the proposed guidelines by identifying their strengths and weaknesses. In total, 28% of the respondents could identify at least one weakness in the proposed guidelines. Common weaknesses identified are frequent reviews needed (several reviews would need to be completed in the future depending on the performance of the results) and specificity (the guideline should offer more specific advice depending on the environment setting and nature of companies' operations). Some respondents appreciated the guidelines that it is risk-based, which would help companies identify and prioritise fixing noted risks and threats effectively.

Significance of the study

The study will enlighten several organizations in Tanzania and elsewhere, including SMEs, on directives to follow to allow their workforce to safely work away from their central offices (remote working), especially during unforeseen pandemics such as COVID-19. It will also help several governments to create and enhance the most applicable policies, controls, frameworks and procedures. The stated measures will enable organisations to overcome some challenges and constraints associated with cybersecurity in remote working and thus ensure the readiness of countries' organizations to switch to remote working normally and leverage available advantages, including increased productivity and cost saving.

Table 5: **Proposed guidelines for cybersecurity by MNOs in remote working**

Code	Process or function	Activity
CI	Cyber-threat Identification	• An organisation needs to investigate to identify the type of attacks. This can be achieved by analysing reports or records of cyber-attack incidences. • The study also needs to quantify each cyber-threat intensity or frequency of occurrence.
AI	Assets identification	• Identify types of assets potentially at risk. • Track assets are moving off-premises (from previously situated on-premises) in inventories.
MA	Matching	• Try to match each cyber threat with the respective control measure(s) available. • Analyse and select the most effective measure for each identified cyber threat.
FE	Financial evaluation	• Evaluate the cost associated with the execution of each cyber-control selected. • Compare the cost analysed with the budget available at the disposal.
PR	Protect	• Analyse how to safeguard all identified assets best. Once the organisation has a grasp of the systems, assets, data, and capabilities in its environment and their associated risks, the next function, protect and guide actions for deciding what specific steps to take to protect them.
DT	Detect	• Define how threats against assets will be detected.
RS	Respond	• The fourth NIST CSF function is based on the fact that no organisation is immune from a cybersecurity event, no matter how proactive it has been, so it is crucial to respond to cybersecurity events. • Outline key measures to respond to detected threats.

CONCLUSION AND RECOMMENDATIONS

The remote working settings for MNOs are often associated with cyber-threat dangers. However, this situation is not only in developing and developed countries. For instance, since COVID-19, the United States (US) - The Federal Bureau of Investigation (FBI) reported a 300% increase in reported cybercrimes. During this period, hackers leveraged the opportunity to attack vulnerable networks as office work moved to personal homes (Devon, 2020). This study finds out the types of cyber-attacks that are predominant to MNOs in remote working and how they occur. In particular, different cyber-attacks were identified for evaluation. Among the identified cyber-attacks, the highly perceived cyber-threat was revealed as human errors followed by phishing attacks, malicious domain, denial of service and ransomware. Human error leads to other cyber threats because making mistakes is a core part of the human experience. Also, in evaluating cyber controls that MNOs are applying to counter cyber breaches, the study found the controls to be VPN, antivirus and backups, staff training, 2FA, remote computer access service and network protocol analyser. A comparison between cyber-attacks reported and cyber control methods applied has brought some uncertainty as the results have revealed the use of VPN has been the most applicable control by MNOs in ensuring cybersecurity in remote working, contrary to what other researchers are suggesting and the fact that human error was identified to be the number one. This indicates a mismatch

between "the cause" and "the control" which could signify inefficiency in cybersecurity management by these organisations. The observed gap indicates a need for guidelines that would ensure effective cyber control based on the intensity of the attacks.

In proposing the guidelines for enhancing cybersecurity in remote working, two frameworks were analysed: NIST and Malaysian, and their strengths and weaknesses enabled us to propose the most suitable guidelines for companies opting for remote working culture. The NIST framework was adapted as follows: the investigation of cyber threats affecting the organisation and their intensity before planning the control measures, then after identifying the control measure(s) to be applied; it is important to evaluate the cost implication of each selected measure(s) to select the feasible method, i.e., within the organisation's capacity. Also, the proposed guidelines considered the importance of implementing control measures based on the identified cyber threats' priority, risk damage, and occurrence rate.

As data breaches become more pervasive in our interconnected world, so must our understanding of modern-day cyber-attacks and controls. Individuals, employees, and organisations must be cyber secure. Therefore, the study provides some important recommendations and suggestions to MNOs and other companies on effective cybersecurity management. These suggestions are based on the nature of the cyber-attacks and control mechanisms identified and analysed. It also provides suggestions for the proposed guidelines that can be used to manage cybersecurity in remote working situations. The study suggests that MNOs should be aware of all types of cyber threats that are more and less likely to occur in remote working, and they must also develop plans or follow up on the proposed guidelines to counter the effects of the noted threats by considering their intensity of occurrence and associated risks. However, since human error is the leading cyberattack in remote working, reducing its occurrence would significantly reduce the overall incidences of cybercrimes. MNOs are advised to invest in providing advanced regular cyber training and education solutions to all their staff regardless of the departments or sections to which they belong. Furthermore, this study would help other companies and organisations in Tanzania identify and enforce appropriate cybersecurity measures that would safely allow their workforce to work from home (remote working) with minimal exposure to cyber risks.

REFERENCES

Acharya, C. (2018), "A Case Study on various Network Security Tools", *International Journal of Modern Trends in Engineering & Research*, **5**(5): 156–161.

Al-Sartawi, A.M.A.M. (2020), "Information technology governance and cybersecurity at the board level", *International Journal of Critical Infrastructures*, **16**(2): 150–161.

Baldini, G., Barrero, J., Chaudron, S., Coisel, I., Draper Gil, G., Duch Brown, N., Eulaerts, O., *et al.* (2020), *Cybersecurity, Our Digital Anchor*, edited by Nai Fovino, I., Barry, G., Chaudron, S., Coisel, I., Dewar, M., Junklewitz, H., Kampourakis, G., et al., Publications Office of the European Union, Luxembourg, available at:https://doi.org/10.2760/352218.

Beyer, R.E. and Brummel, B.J. (2015), "Implementing effective cyber security training for end users of computer networks", *SHRM-SIOP Science of HR Series: Promoting Evidence-Based HR*.

Chbib, A. (2021), "The Cybersecurity Challenges of Remote Work", available at: https://www.linkedin.com/pulse/cybersecurity-challenges-remote-work-anas-chbib (accessed 20 April 2022).

Chou, C.C., Lee, C., Tao, X., Qian, Z. and Tacheva, J. (2022), "The effects of use of multiple social media platforms on firm performance: An empirical study", *International Journal of Management and Decision Making*, **21**(2): 129–143.

Devon. (2020), "15 alarming cyber security facts and stats", *Cybint Customer DPA*, available at: https://www.cybintsolutions.com/cyber-security-facts-stats/ (accessed 28 May 2022).

Durbin, S. (2021), "Top 5 cybersecurity challenges in the hybrid office", *BNP Media*, available at: https://www.securitymagazine.com/articles/95434-top-5-cybersecurity-challenges-in-the-hybrid-office (accessed 20 April 2022).

Di Gennaro, F., Pizzol, D., Marotta, C., Antunes, M., Racalbuto, V., Veronese, N. and Smith, L. (2020), "Coronavirus diseases (COVID-19) current status and future perspectives: A narrative review", *International Journal of Environmental Research and Public Health*, **17**(8): 1-11 available at:https://doi.org/10.3390/ijerph17082690.

Jain, J. and Pal, P.R. (2017), "A Recent Study over Cyber Security and its Elements", *International Journal of Advanced Research in Computer Science*, **8**(3): 791–793.

Kechagias, E.P., Chatzistelios, G., Papadopoulos, G.A. and Apostolou, P. (2022), "Digital transformation of the maritime industry: A cybersecurity systemic approach", *International Journal of Critical Infrastructure Protection*, **37**:1–14.

Kertysova, K., Frinking, E., Dool, K. van den, Maričić, A. and Bhattacharyya, K. (2018), *Cybersecurity : Ensuring Awareness and Resilience of the Private Sector across Europe in Face of Mounting Cyber Risks*, The European Economic and Social Committee (EESC), The Netherlands, available at:https://doi.org/10.2864/98090.

Maganga, D.P. and Taifa, I.W.R. (2022), "Quality 4.0 conceptualisation: an emerging quality management concept for manufacturing industries", *The TQM Journal*, available at:https://doi.org/10.1108/tqm-11-2021-0328.

Malatji, M., Marnewick, A. and von Solms, S. (2020), "Validation of a socio-technical management process for optimising cybersecurity practices", *Computers and Security*, **95**: 101846.

Medromi, H., Sayouti, A. and Faris, S. (2014), "The Impact of Cyber Security Issues on Businesses and Governments : A Framework for Implementing a Cyber Security Plan", *2014 International Conference on Future Internet of Things and Cloud*, IEEE, Barcelona, Spain, available at:https://doi.org/10.1109/FiCloud.2014.56.

Morze, N. and Smyrnova-Trybulska, E. (2021), "Web-based community-supported online education during the COVID-19 pandemic", *International Journal of Web Based Communities*, **17(**1): 9–34.

Moturi, C.A., Abdulrahim, N.R. and Orwa, D.O. (2021), "Towards adequate cybersecurity risk management in SMEs", *International Journal of Business Continuity and Risk Management*, **11**(4): 379–396.

Mwasubila, I.J., Taifa, I.W.R. and Kundi, B.A.T. (2022), "An analytical study on establishing strategies for improving the productivity of the spinning industries", *International Journal of Industrial and Systems Engineering*, **40**(1): 1–28.

Nabe, C. (2020), "Impact of COVID-19 on Cybersecurity", *Delloite Switzerland*.

Nchalala, A., Alexander, T. and Taifa, I.W.R. (2022), "Establishing standard allowed minutes and sewing efficiency for the garment industry in Tanzania", *Research Journal of Textile and Apparel*, available at:https://doi.org/10.1108/RJTA-09-2021-0112.

Owens, L.K. (2002), *Introduction to Survey Research Design*, SRL Fall 2002 Seminar Series, New York, NY, USA.

PAC. (2013), *Competitive Analysis of the UK Cyber Security Sector*, Pierre Audoin Consultants (PAC) UK Ltd, UK.

Ponemon Institute. (2020), *Cybersecurity in the Remote Work Era: A Global Risk Report*, Ponemon Institute LLC, Michigan, USA, available at: https://www.keeper.io/hubfs/PDF/Cybersecurity in the Remote Work Era - A Global Risk Report.pdf.

Radhakrishna, R., Tobin, D., Brennan, M. and Thomson, J. (2012), "Ensuring data quality in extension research and evaluation studies", *Journal of Extension*, **50**(3).

Sadri, M.J. and Asaar, M.R. (2021), "An anonymous two-factor authentication protocol for IoT-based applications", *Computer Networks*, **199**, 1–12.

Salamzada, K., Shukur, Z. and Abu Bakar, M. (2015), "A Framework for Cybersecurity Strategy for Developing Countries: Case Study of Afghanistan", *Asia-Pacific Journal of Information Technology and Multimedia*, **04**(01): 1–10.

Senarak, C. (2021), "Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel", *Asian Journal of Shipping and Logistics*, **37**(4): 345–360.

Sheshadri, V. (2022), "NIST framework: 5 pillars for your cyber security strategy", *RiverSafe Ltd*.

Shuster, C. (2021), "Top 50 NIST CSF Tips to Address Remote Work Cybersecurity Risk", *Axio Global, Inc*.

Sposato, M. (2021), "Remote working in the time of covid-19: Developing a web-based community", *International Journal of Web Based Communities*, **17**(1): 1–8.

Taifa, I.W. (2016), *Integration of Quality Function Deployment (QFD) and Ergonomics Principles in Product Design Improvement. Case Study: Student Desk at Engineering College*, Master's Dissertation, Gujarat Technological University, Ahmedabad.

Taifa, I.W.R., Hayes, S.G. and Stalker, I.D. (2020), "Computer modelling and simulation of an equitable order distribution in manufacturing through the Industry 4.0 framework", *2nd International Conference on Electrical, Communication and Computer Engineering (ICECCE), 12-13 June 2020*, IEEE, Istanbul, Turkey: 1–6.

Taifa, I.W.R., Hayes, S.G. and Stalker, I.D. (2021), "Towards a digital revolution in the UK apparel manufacturing: An industry 4.0 perspective", in Bartolo, P., Silva, F., Jaradat, S. and Bartolo, H. (Eds.), *Industry 4.0 – Shaping the Future of the Digital World, 2nd International Conference on Sustainable Smart Manufacturing (S2M 2019), Manchester*, CRC Press, Taylor & Francis Group, London, UK: 3–8.

TCRA. (2021), *Quarterly Communications Statistics: April - June 2021*, The Tanzania Communications Regulatory Authority (TCRA), Dar es Salaam, available at: https://www.tcra.go.tz/uploads/text-editor/files/TelCom Statistics June 2021_1630483653.pdf.

Wessels, M., van den Brink, P., Verburgh, T., Cadet, B. and van Ruijven, T. (2021), "Understanding incentives for cybersecurity investments: Development and application of a typology", *Digital Business*, **1**(2): 100014.