International Journal of Multidisciplinary and Current Educational Research (IJMCER)
ISSN: 2581-7027 ||Volume|| 6 ||Issue|| 2 ||Pages 143-150 ||2024||

Impact of Remote Work Technology on Employee Performance: A Case of Dodoma University, Tanzania

[1,]Cedric Samson Chipwaza, [2,]Adam Aloyce Semlambo
Department of Informatics - Institute of Accountancy Arusha (IAA), Tanzania.

ABSTRACT : The introduction of technology and the developing nature of the modern workforce have resulted in a significant change in traditional work arrangements. The increasing popularity of remote and teleworking is challenging the traditional office-based approach. This study investigates the impact of digital technology on employee performance in a remote work environment at Dodoma University. The study employed a case-study research design with both qualitative and quantitative approaches. The target population was the management, teaching, and teaching staff of Dodoma University. A sample size comprised 335 respondents. The data collection tools included questionnaires and individual, in-depth interviews. SPSS was employed as the data analysis tool. The results showed that over 68% of respondents used Zoom daily to work remotely. On the other hand, the study found that the most common cyber threats that affect remote work environments are malware, denial of service (DoS), social engineering, and insider threats. Furthermore, the study concluded that these cyber threats could be blocked by implementing security measures like strong passwords, changing passwords often, using antivirus software, blocking spam users, and setting login alerts when using online platforms to share content. Moreover, the findings revealed that adopting digital technologies positively impacts employees' performance in a remote work environment. The study recommended that Dodoma University implement technology management strategies that address digital distractions. This could involve providing guidelines on managing notifications and promoting focused work periods to mitigate the negative impact of distractions on performance. The university should prioritise developing and implementing remote training programs tailored to address specific skill gaps relevant to remote work scenarios.

KEY WORDS: Digital Technology, Remote work, Dodoma University, Cyberthreats, Cybersecurity

I. INTRODUCTION

The introduction of technology and the developing nature of the modern workforce have resulted in a significant change in traditional work arrangements. The traditional office-based approach is being challenged by the increasing popularity of remote working and teleworking (Chanana & Sangeeta, 2021). Remote work has become popular in recent years due to the various advantages it offers organisations (Gonzalez, 2020). One of the main advantages is more flexibility. Working remotely from anywhere can improve work-life balance and job satisfaction (Peasley et al., 2020). Following the recent COVID-19 pandemic since 2020, a significant percentage of the workforce has shifted to working remotely (Wang et al., 2021). The widespread use of digital technology to make it possible has highlighted the importance of digital technology in enabling remote working (Ozimek, 2020).

The COVID-19 pandemic has accelerated the global adoption of remote working practices by compelling businesses to enforce social distancing measures to safeguard their employees' health and maintain business continuity (World Health Organization, 2020). The increasing adoption of remote working practices in organisations has raised questions about their impact on employee performance. While remote work offers benefits such as flexibility and improved work-life balance (Gonzalez, 2020), it also presents unique challenges related to communication, collaboration, and employee engagement (Golden, 2020). However, remote working can positively or negatively impact employees' performance within an organisation. It can reduce costs by freeing up resources, improving efficiency, boosting employee motivation, and ultimately leading to higher productivity (Peasley et al., 2020). Soni, Kukreja, and Sharma (2020) argued that the best practices and policies for employees' environments would not be compliant due to the fast transition to a remote work environment. This lack of preparedness and wide use of technology put organisations and employees in a vulnerable position regarding cybersecurity. This is evidenced by the Global Risk Report of 2022, which states that in 2020, malware and ransomware increased by more than 35% for both categories (World Economic Forum, 2022). Furthermore, the same report stated that most cybersecurity issues are due to human error, for example, insider threats, which can be intentional or unintentional. Educational institutions, including Dodoma University, have swiftly transitioned to remote working to uphold their academic and administrative operations while prioritising the safety of their staff. However, this rapid shift to remote working has exposed organisations to potential security risks and data protection challenges (Mtebe et al., 2021). As employees access organisational networks and sensitive information from outside the secure office environment, the risk of cyber threats and breaches increases, potentially compromising the confidentiality, integrity, and availability of valuable assets (Ibrahim et al., 2020). Furthermore, the university staff, especially during COVID-19, prefer to communicate and facilitate online lectures through Zoom and other social networking sites like WhatsApp and Telegram (Mtebe et al., 2021). This exposes the organisation to a high risk of cyber threats, where hackers could attack sensitive information shared on online platforms through social engineering (Ibid.). Therefore, there is a need to understand the unique dynamics of remote work and its influence on employee performance, specifically at Dodoma University. To address this research gap, this study examined the impact of remote working best practices on employee performance at Dodoma University.

II. LITERATURE REVIEW

Theoretical Review : This study employed Social Exchange Theory: This theory was designed by American sociologists Homans (1910–1989) and Blau (1918–2002). This theory explains people's behaviour when exchanging information on online platforms. It studies human behaviour according to situations (Lawler& Thye, 2006). This theory is based on three fundamental concepts: Costs, which encompass various expenditures such as time, effort, or money (Lawler& Thye, 2006); Rewards, which encompass a range of benefits like acceptance, support, or companionship (Lawler, 2001); and Resources, which can be any material or symbolic commodities transmitted through interpersonal interactions, endowing individuals with the capacity to reward others. While Social Exchange Theory has some weaknesses, such as its often-romantic relationship orientation and the oversimplified linear model of relationships (Miller, 2005), it remains highly relevant to this study. It provides valuable insights into how people's behaviour can influence information disclosure on social networks. However, this theory is relevant to the current study as it explains how people's behaviour can result in cyber threats in digital communication, hence affecting employee performance in the organisation. Moreover, the theory analyses the costs and benefits of sharing personal information on digital platforms, which may influence the privacy and security of an organisation’s sensitive data.

Empirical Review : Pranggono and Arabo (2021) stated that many organisations did not have a procedure to build a remote workforce in the UK. The authors also observed that only 38% of organisations had a security policy. Similarly, Naidoo (2020) indicated that organisations' most important priority was facilitating employees’ working remotely quickly. Consequently, the authors emphasised that the organisation lacked time to build and deploy the correct security safeguards. Pranggono and Arabo (2021) stated that, in many cases, employees used their home systems to perform their jobs. The employer secured these systems, but this new infrastructure created a clear security concern. According to Alexander and Jaffer (2021), existing safeguards such as the Virtual Private Network (VPN) and other organisational tools still contain vulnerabilities. The literature suggests an inherent vulnerability in the current remote work practices. In addition, there is a clear increase in dependency on technology from organisations (Naidoo, 2020), which cybercriminals have not overseen, and the number of cybercrimes has been observed to have grown significantly. Naidoo (2020) also observed that emotional factors can be important in users’ compliance with security policies. It is important to mention that these attacks are not necessarily new; they have just been repeatedly exploited in this era. Malware, including phishing or ransomware, DDoS, and misinformation, are among the most commonly used cyberattacks during COVID-19.

Furthermore, according to the Center for the Protection of National Infrastructure (CPNI, 2020), remote work's complexity can generate insider threat attacks. This is because of multiple factors: oversight from management, an unfamiliar environment, stress, and poor screening processes when adding new employees to the organisation. The success of malware and phishing emails, for example, resides in attackers using current relevant information, in this case, related to the pandemic, and using it to attract users with their malicious software (Naidoo, 2020). Furthermore, Pranggono and Arabo (2021) observed that DDoS attacks focused on infrastructure and organisations that were vulnerable or overwhelmed during the pandemic. As an example of these organisations, Pranggono and Arabo (2021) claimed that the Internet or healthcare providers were the targets. According to their study, the reason for this is that this type of organisation’s focus was set on priorities other than cybersecurity, opening a window for vulnerability. Ultimately, we see that users’ increased engagement with technology left the door open for vulnerabilities to be exploited by criminals. As a result of this work environment change, it is worthwhile to consider aspects beyond cybersecurity, which may affect its successful implementation. Galanti et al. (2021) stated that remote work presents some personal challenges for users. First, a family conflict impacts work. Second, social isolation, and third, the distracting environment that users may be in. The importance of this is that, as stated previously, emotional factors may affect cybersecurity compliance on the part of the users.

In addition, envisioning a return to a previous work environment and IT settings would not be appropriate. Still, the new working conditions allow organisations to explore different options. Kane et al. (2021) observed that organisations can take advantage of the effectiveness of remote work. The authors suggested a hybrid model that can provide the flexibility needed in a post-pandemic reality.While numerous studies have explored the impact of remote working best practices on employee performance in developed and developing countries, other scholars, like Farooq and Sultana (2021) and Afshar (2020), demonstrated no correlation between remote work and employee performance. Others, like Atstaja et al. (2021), found that companies and organisations adopting remote work may result in cyber risk management, depending on the nature of the information processed. In Tanzania, there are no clear statistics on the studies done on the impact of remote working best practices on employee performance. Therefore, the current study examined the impact of remote working best practices on employee performance using the case of Dodoma University to fill the existing gap.

III. METHODOLOGY

This study employed a case study research design since it allows an in-depth investigation of one or more examples of a current social phenomenon (Kothari, 2019). Both qualitative and quantitative approaches were used to provide a comprehensive perspective. Quantitative research was chosen for its ability to delve deeply into the study problem (Kothari, 2019), while the qualitative approach was included due to its flexibility and significance in developing more comprehensive data relationships (Creswell, 2014). This study's target population included management staff and other staff within Dodoma University. The university website updates show that the institution has 1517 employees (www.udom.ac.tz, 2024). Administratively, the institution is divided into three directorates: Vice Chancellor (VC), Deputy Vice Chancellor-Academics Research and Consultancy (ARC), and Deputy Chancellor-Planning Finance and Administration (PFA).

The sample size was obtained based on Taro Yamane's mathematical model (1967). The formula used was:

$n = N / (1 + Ne^2)$

Where: n = sample size N = population size 1497(After deducting 20 key informants using saturation point), e = level of significance or error term (0.05)

$$n = \frac{1497}{1 + 1497\ (0.05^2)} = 315$$

Therefore, the total sample size comprised 335 respondents, including 315 for quantitative and 20 for qualitative data. The sample size for quantitative data comprised 315, including 60 management staff and 255 teaching and non-teaching staff, as summarised in the table below.The study employed questionnaires and individual in-depth interviews as the primary data collection instruments. The questionnaire consisted of only closed-ended questions to gather quantitative information on the magnitude of issues. The interview was conducted with 20 selected staff from the departments that applied for remote work, especially during COVID-19. The data collected underwent coding and editing to identify and rectify errors. With the aid of Microsoft Excel, the Statistical Package for Social Science (SPSS) was employed for data analysis due to its user-friendliness and capability to compute large datasets (Kumar, 2019). Data were presented through frequency tables and charts. Content analysis was used to analyse qualitative data collected through in-depth interviews.

To ensure the validity of the data instruments, a pre-test of the questionnaire with 10 respondents was conducted in the study area. Additionally, to achieve the reliability of this study, Cronbach's alpha was used to determine the reliability of the instrument by establishing how the study variables related to each other.

IV. RESULTS

In this study, 180 of the 315 questionnaires distributed to the respondents within Dodoma University were filled out and returned, 60 were filled out but not properly, and the remaining 75 were not returned at all, yielding a response rate of 57.1%.

Awareness of cybersecurity in the remote working environment

Software tools often used for remote work : The findings revealed that most respondents over the third quarter (68%) indicated that they used Zoom daily when working remotely, 56% said they used Zoom a few times per week, and the same percentage said they used Microsoft Teams daily. About 48% of respondents said they used Microsoft Teams every day. Most Dodoma staff utilise Zoom and Microsoft Teams in remote work environments. The results are well presented in Figure 1. During the interview, the majority of the respondents informed the researcher that when they were working at home, especially during COVID-19, they used Zoom most of the time to perform some of their duties, including lectures with postgraduate students (masters and PhD students).

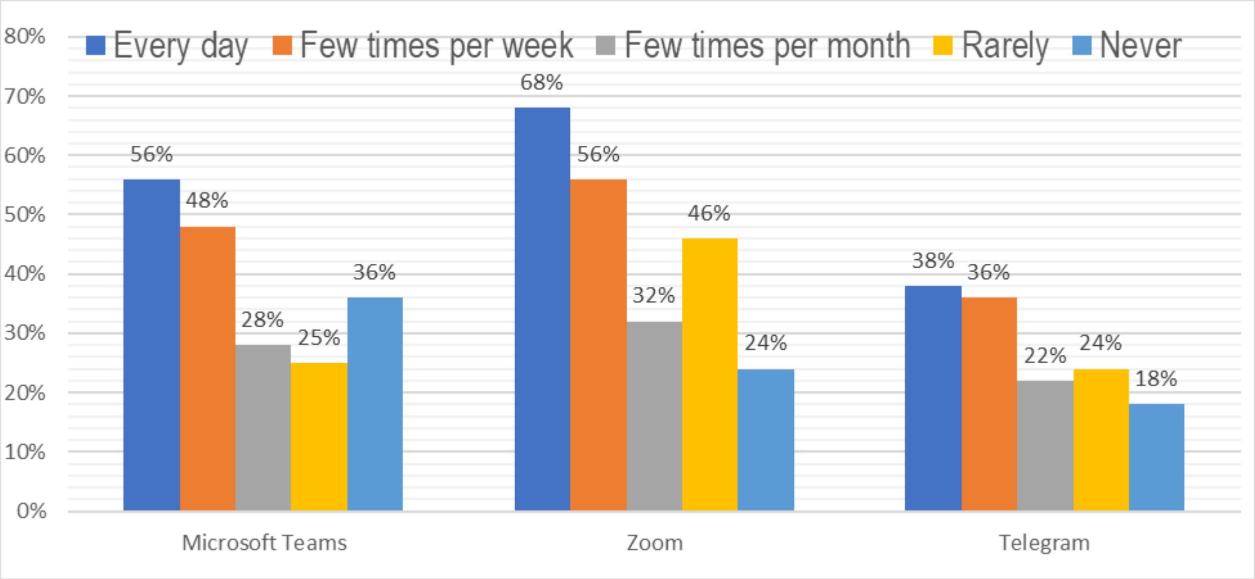

Figure 1: Software tools for remote work
Source: Field Data (2024)

Staff awareness of cybersecurity in the remote working environment : The results revealed that most of the respondents (over 82.2%) contended that they are aware of the use of strong passwords, but only 37.2% use the strategy of changing passwords occasionally. This implies that the third quarter of the respondents were aware of only using passwords as key measures to protect their data sharing in a remote work environment. During the interview, some respondents said that most people in public institutions have inadequate ICT and cybersecurity skills in general, which is why it is easy for the organisation's computerised systems, such as websites and other online resources, to be attacked by hackers.

Table 1: Staff awareness of cybersecurity.

Statement	Frequency	Percent
Use of strong password	148	82.2
Changing password often	67	37.2
Use of information disclosure	52	28.8
Use of antivirus software	45	25
Set the control on how others can find you	31	17.2
Block Spam Users	22	12.2
Set login Alerts	8	4.4

Source: Field data (2024)

The findings revealed that only a few of the respondents, less than half, are aware of other cybersecurity protective measures such as antivirus software, control over how others can find you, blocking spam users, and login alerts. This means that staff working remotely are not effectively using antivirus software to protect the organisation's data on their devices. This creates a loophole for malicious attacks to hack the devices and access the office-stored data.

Cyberthreats in a Remote Work Environment : The respondents were asked to indicate cyber threats in a remote work environment. The findings noted that over three-quarters mentioned at least four threats, as illustrated in Table 2 below.

Table 2: Type of Cyberthreats in a Remote Work Environment

Security Threats	Frequency	Percent
Social Engineering	84	46.7
Insider Threat	58	32.2
Malware	116	64.4
Denial of Service (DoS)	88	48.9
Phishing	48	26.7

Source: Field data (2024)

The results revealed that most respondents (over 64%) were aware of malware threats, followed by 48.9% who mentioned denial of service (DoS). While 46.7% of the respondents said social engineering and 32.2% mentioned insider threats. However, during the interview, some of the respondents (staff with remote working experience) demonstrated that there is a risk of unauthorised access to work resources and access to high-risk Internet resources through cyberattacks like phishing and social engineering when a device used for remote working settings is utilised by another household (for example, for distance learning or Internet browsing). Respondents who indicated that peers also utilise devices for remote working use both work and private devices.

Impact of Remote Work Technology on Employee's Performance : Employees reported being distracted by digital technology while working in a remote environment (mean = 2.31, STD = 1.19), indicating a generally positive attitude toward working in a remote area. Respondents largely indicated that digital technology has affected their ability to work independently at home (mean = 3.18, standard deviation = 1.12), suggesting that many employees find comfort in using digital technology while working remotely. A significant majority of respondents (mean = 3.02, STD STD=1.28) demonstrated a strong grasp of their assigned tasks after receiving sufficient training on how to use digital technology effectively for work-related tasks. The data indicated that many employees believed digital technology made their work more efficient while working from home (mean = 3.48, STD = 1.26), underscoring the perceived advantages of a remote work environment for focused work. Furthermore, the data revealed that most respondents reported that digital technology has enhanced cohesion between family and work life (mean = 3.25, STD = 1.18), indicating a level of adaptability to remote work environments through digital technology. Lastly, the majority of respondents (mean = 4.1, STD = 0.969) reported that they use digital technology to communicate with their colleagues in the workplace and maintain performance while working remotely.

Table 3: Descriptive Statistics for Digital Technology and Employee Performance

Statement	N	Mean	STD
I feel distracted by digital technology while working	180	2.31	1.19
Digital technology has affected my performance at work.	180	3.18	1.12
I have received sufficient training on how to use digital technology effectively for work-related tasks.	180	3.02	1.28
Digital technology has made my work more efficient.	180	3.48	1.26
Digital technology has enhanced cohesion between family and work life.	180	3.25	1.18
Digital technology supports my communication with colleagues.	180	2.75	1.34

Source: Field Data (2024)

Correlation Analysis of Digital Technology and Employee Performance : A correlation analysis was carried out to determine if a correlation existed between digital technology and employee performance. Table 4.6 below summarises the results of the analysis. The findings revealed a positive correlation between digital technology and employee performance (r=0.32). Implies that employee performance increases with an increase in digital technology.

Table 4: Correlation Analysis of Digital Technology and Employee Performance

Variable	N	Digital Technology	Employee Performance
Digital Technology	180	1.00	0.34
Employee Performance	180	0.34	1.00

Source: Field Data (2024)

Regression Analysis for Digital Technology and Employee Performance : The research analysed the relationship between digital technology and employee performance based on Table 4.7 below. The results showed that the adjusted R^2 value was 0.004369649; hence, 0.415% of the variation in Employee performance was explained by digital technology.

Table 5: Regression Analysis of Digital Technology Influence on Employee Performance

Regression Statistics: Model Summary	
Multiple R	0.064566545
R Square	0.004369649
Adjusted R Square	-0.00516182
Standard Error	1.19659319
Observations	180

Predictors: (Constant), Digital technology
Source: Field Data (2024)

V. DISCUSSION

Awareness of cybersecurity in remote working environments : The findings from our study reveal a significant awareness gap in cybersecurity practices among Dodoma University staff, with a notable reliance on basic measures such as password usage. While 82.2% of respondents recognised the importance of strong passwords, far fewer acknowledged the necessity of comprehensive cybersecurity measures, such as antivirus software, control over personal visibility online, blocking spam users, and setting login alerts. This aligns with Atstaja et al. (2021), who observed that remote workers often lack awareness of system and technological risks, particularly those associated with third-party platforms, and fail to implement stringent protective measures on their devices and systems. This gap facilitates attackers' ability to manipulate information or capture data, highlighting the critical need for data encryption and stricter policy enforcement on free services. Echoing these concerns, an interviewed staff member stated, "We often focus on remembering our passwords, but I think there's more we could be doing. I'm not fully aware of how to protect against other threats and unsure if I'm doing enough." This sentiment underscores a broader trend of uncertainty and potential complacency in adopting more advanced cybersecurity practices.

Furthermore, Ngere (2022) emphasised that the transition to remote work has amplified organisations' need to reassess their security procedures, especially concerning data access from remote locations. This external access introduces heightened risks of data leakage and other security breaches, necessitating stringent organisational regulations and procedures to mitigate data loss. "Our biggest challenge isn't just about using strong passwords; it's about ensuring that our entire remote setup is secure. I'm concerned about the security of our network and the potential for data leaks," shared another respondent, reflecting the critical need for a holistic security approach.Despite the availability of numerous prevention and detection solutions, such as firewalls, VPNs, IDS, and IPS, their effectiveness is contingent upon a robust legal framework. Michaelides (2021) notes that remote workers' use of various unsecured communication channels, such as emails and instant messaging, can undermine these measures. This observation is particularly relevant to our findings, where a lack of comprehensive cybersecurity awareness could lead to non-compliance with data processing and management standards. An interviewed administrator remarked, "We have implemented VPNs and firewalls, but I worry about our staff's use of personal devices and email for work. It is difficult to ensure they are always secure."

Flores et al. (2023) advocate for implementing Data Loss Prevention (DLP) solutions, highlighting the critical role of enforcing security standards for data processing, classification, and management. Our findings suggest that while some staff members at Dodoma University are aware of and utilise basic cybersecurity measures, a considerable gap exists in adopting a comprehensive cybersecurity framework, as evidenced by the lack of widespread use of antivirus software, spam user blocking, and login alerts.

Impact of Remote Work Technology and Employee Performance : Our findings illuminate digital technologies' significant positive impact on employee performance in remote work environments. Notably, the data indicated that digital technology facilitates communication among colleagues, with most respondents (mean = 4.1, STD = 0.969) affirming its role in maintaining performance standards while working remotely. This supports Oliver's (2018) observation that technology-mediated communication, despite its potential to disrupt workflow, primarily enhances productivity over time by making communication more straight forward. However, Taylor and Brown (2018) and Blount (2015) offer a complementary perspective, suggesting that the effectiveness of digital technology in enhancing job satisfaction and task efficiency hinges on its thoughtful implementation within organisational structures. "The shift to remote work necessitated an overhaul in how we approach our tasks. With the right tools, we have not only maintained but, in some cases, improved our efficiency," shared a respondent, highlighting the transformative impact of digital tools when appropriately utilised.

White et al. (2020) delve into the individual variation in technological adaptation, revealing a spectrum of employee responses to digital distractions. From our interviews, a staff member reflected, "While I find certain notifications disruptive, I have learned to leverage technology to prioritise and multitask more effectively." This statement underscores the importance of recognising and addressing individual differences in technological engagement and the potential for digital tools to enhance multitasking capabilities when managed well.The qualitative insights from our interviews echo Jalagat and Jalagat's (2019) assertion of digital technology's fundamental role in supporting remote work. Conversely, Elshaiekh Hassan and Abdallah's (2018) contention that remote work can negatively impact performance highlights the necessity for a balanced view. "Working from home has its challenges. Distractions are plentiful, and the boundary between work and home life blurs easily," remarked another interviewee, indicating the nuanced reality of remote work's impact on performance.

Cheruiyot (2015) further emphasises the potential of digital technology to enhance remote work environments, provided its application is properly managed. Our study participants shared varied experiences, with one noting, "The adoption of digital tools has been a game-changer for us. It is not just about staying connected but about being more productive and efficient in ways we had not anticipated."

VI. CONCLUSIONS AND RECOMMENDATIONS

Conclusions : The study revealed a positive correlation between digital technology and employee performance, signifying that heightened digital technology adoption is linked to increased employee performance. However, the study revealed that remote working technology could be hampered by cyber threats such as malware threats, denial of service (DoS), and social engineering, and 32.2% mentioned insider threats. The study concludes that digital technologies positively impact employee's performance in the remote work environment by helping employees communicate with their colleagues and maintain organisational performance while working remotely.

Recommendations: The study encourages the essential use of security measures like strong passwords, changing passwords often, using antivirus software, blocking spam users, and setting login alerts when using online platforms for sharing content. Considering the positive correlation, organisations should focus on enhancing the remote working environment to boost employee performance further. Dodoma University should consider implementing technology management strategies that address digital distractions. This could involve providing guidelines on managing notifications and promoting focused work periods to mitigate the negative impact of distractions on performance. The university should prioritise developing and implementing remote training programs tailored to address specific skill gaps relevant to remote work scenarios. The organisation should ensure that these programs offer practical skills directly contributing to task efficiency and job performance.

REFERENCES

1. Afshar, V. (2020). Working from home: The future of business is remote. https://www.zdnet.com/article/the-average-productivity-loss-of-remote-work-is-1/

2. Almaamari, Q. A., & Alaswad, H. I. (2021). Factors Influencing Employees' Productivity- Literature Review. Turkish Online Journal of Qualitative Inquiry, 12(6).

3. Aropah, V. D. W., Sarma, M. M., & Sumertajaya, I. (2020). Factors Affecting Employee Performance during Work from Home. International Research Journal of Business Studies, 13(2)

4. Atstaja, L., & Rutitis, D., & Deruma, S., & Aksjonenko, E. (2021). Cyber Security Risks and Challenges In Remote Work Under The Covid-19 Pandemic

5. Chanana, N., & Sangeeta. (2021). Employee engagement practices during COVID-19 lockdown. Journal of public affairs, 21(4), e2508.

6. Creswell, J. (2019). Research Design: Qualitative, Quantitative and Mixed Methods Approaches. Thousand Oaks, CA: Sage

7. Farooq, R. & Sultana, A. (2021). The potential impact of the COVID-19 pandemic on work from home and employee performance. Measuring Business Excellence, 10, 11-23

8. Flores, C., & Gonzales, J., Kajtazi, M., & Bugeja, J., & Vogel, Br. (2023). Human Factors for Cybersecurity Awareness in a Remote Work Environment. 608-616. 10.5220/0011746000003405.

9. Gonzalez, L. (2020). The Effects of COVID-19 on Productivity in Project Management. McGraw Hill.

10. Ibrahim, G., Luzinga, H., & Kapanda, G. (2020). Teaching and learning experiences in medical education during the COVID-19 pandemic: The case of Kilimanjaro Christian Medical University College (KCMUCo), Tanzania. Journal of Learning for Development, 7(3), 433–446.

11. Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. King's College London and Ipsos Mori. (2020). Life under lockdown: coronavirus in the UK. King’s College London. https://www.kcl.ac.uk/policy-institute/assets/coronavirus-in-the-uk.pdf

12. Kothari, C.R. (2019). Research Methodology: Methods and Techniques. 4th Edition, New Age International Publishers, New Delhi.

13. Kumar, R. (2019). Research methodology: A step-by-step guide for beginners: Sage Publications Limited.

14. Michaelides, N. (2021). Remote Working and Cyber Security Literature Review.

15. Mtebe, J. S. (2020). An Investigation of eLearning System SelfEfficacy amongst instructors at the University of Dodoma, Tanzania. Open Praxis, 12(3), 343–357. https://doi.org/10.5944/openpraxis.12.3.1103

16. Mtebe, J. S., Fulgence, K., & Gallagher, M. S. (2021). COVID-19 and Technology Enhanced Teaching in Higher Education in sub-Saharan Africa: A Case of the University of Dar es Salaam, Tanzania. Journal of Learning for Development (JL4D), 8(2), 383–397. https://jl4d.org/index.php/ejl4d/article/view/483/ 647

17. Ngere D_A.(2022). Cybersecurity Assessment of the Remote Working Environment During Covid-19 A Case Study of Financial Regulators in Kenya

18. Okereafor, K., & Adebola, O. (2020). Tackling the Cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety. Journal Homepage: http://ijmr. net. in, 8(2)