NATIONAL BOARD FOR TECHNICAL EDUCATION
NATIONAL JOURNAL OF TECHNICAL EDUCATION
Volume 24 Nos. 1 2025
ISSN No. 2992-3522

Cyber Security Hurdles Confronting Employees within Nigeria Digital Workplaces

*Adebayo Ademola Riliwan[1], Sholanke Oluwafunmbi Benedict[1], Ogunode Rotimi Samuel[1] and Elekula Oluwafemi Idowu[1]

[1]Computer Science Department, Federal School of Surveying, Oyo
[1]**Email:** aadebayo22@yahoo.com

Abstract

Businesses are integrating information and communication technology (ICT) and in their operations in other to ensure survival within Nigerian digital workplaces. However, this reliance on technology presents challenges, as it is susceptible to attacks stemming from both technical vulnerabilities and human errors. Human factors, in particular, pose significant obstacles for organizations, given their complex nature and the predominant role humans play in cybersecurity incidents. Therefore, research to explore the cybersecurity challenges faced by employees of digital organizations in Nigeria's digital workplace was carried out.

Qualitative research and semi-structured interviews were employed to gather data from 50 individuals working in different digital firms across Nigeria. Thematic analysis was utilized to analyse the data, revealing six prominent themes: lack of adequate knowledge and training, deficiencies in passwords and authentication, the impact of bring-your-own-device (BYOD) policies, insider risks, vulnerabilities to social engineering attacks, and the challenges associated with remote work. Subthemes were further infer based on participant response.

The findings highlight the extent to which employees in Nigerian digital workplaces lag in cybersecurity awareness and preparedness, underscoring the need for concerted efforts to address these issues effectively. This paper provides an overview of cybersecurity challenges encountered by Nigeria's digital workers and lays a foundation for future regional cybersecurity research endeavours.

Keywords: cyber security, digital workplace, Nigeria, human errors

Introduction

In today's fiercely competitive landscape, safeguarding against threats that emanated from internet has emerged as a priority for users, particularly in the intricacies of digital environments (Al Nafea & Almaiah, 2021). Insufficient employee awareness and knowledge regarding these threats significantly elevate the risk of business digitization to cyberattacks (Humayun *et al.*, 2020). Nigeria with its developing economy and giant of Africa, Nigeria's digital workplace experiences various cybersecurity challenges. Studies have provided additional support for this argument (Ajufo & Qutieshat, 2023; Ogunyemi, & Idowu, 2023; Oloidi, 2019).

The rise in business digitalization has heightened the imperative for firms to protect themselves from cyber threats (Tweneboah-Koduah, Skouby, & Tadayoni, 2017). Previous research focused on developed nations, such as Europe and America, regarding cybersecurity challenges employee encounter in the digital workplace. In the case of Apostolopoulos et al. (2021), malware, weak passwords, and phishing attacks were identified as cybersecurity challenges faced by employees in the Europe. Similarly, Back and Guerette (2021) found that attacks from phishing activities and weak passwords are top of the cyber security challenges employees faced in developed countries.

Nevertheless, there is low output of research on cybersecurity obstacles encounter by employees in developing regions like Nigeria and Africa. In 2003, according to the National Cyber Threat Forecast, the Cyber Security Experts Association of Nigeria (CSEAN) mentioned that low level of awareness and training coupled with insider threats and social engineering attacks are predominant cybersecurity challenges faced by both private and public sectors in Nigeria. Highlighted in the report are benefits of sensitising employees in addressing these challenges. However, research on cybersecurity challenges in developing economies which may be caused by cultural, social and economic factors is lacking. This research focused on cybersecurity hurdles confronting Nigeria digital business employees and identifies practical solutions to address them.

The cyber challenges as regard to Nigeria space have been identified as a gap in the literature and should be research into as the country is one of Africa’s fastest-growing digital economies with increasing workplace digitalization. In 2022, the Nigeria Communication Commission

(NCC) projected that internet consumers to reach 60M (65% penetration rate) by 2025 in the country.

In the digital workplace, employees encounter various cyber obstacles that are crucial to address for the security of Nigeria's organizations and its digital settings. Employees are exposed to cyber threats based on reliance on technology and connectivity, highlighting the importance of understanding and mitigating these challenges. Critical infrastructure and sensitive information protection as well as upholding stakeholder confidence are all contingent upon effectively managing cyber risks. By addressing these challenges, organizations can mitigate loss, improve operation, adhere to regulations and foster cyber-resilient culture among stakeholders. The research was structured into five main sections as follows: introduction, review of related work, methodology, data analysis and interpretations, lastly, discussion and future directions. This approach allows for a thorough exploration of cybersecurity issues in Nigeria's digital workplaces and provides a framework for addressing them effectively in the future.

However, cyber threats are not limited to human error but also include technical vulnerabilities within the system. Traditional cryptographic methods such as elliptic curve cryptography (ECC) and Rivest-Shamir-Adleman (RSA) face significant threats due to their vulnerability to quantum attacks thereby leading to the advent of post-quantum cryptography (PQC). Quantum computers are said to efficiently solve problems that are currently infeasible for classical computers (Anastasova, Azarderakhsh, & Kermani, 2022). In their work, a new record for the SIKE protocol was presented by implementing novel low-level finite field arithmetic targeting the ARMv7-M architecture. Supported by Canto, Sarker, Kaur, Kermani, & Azarderakhsh (2022), error detection schemes for multipliers in lattice-based key encapsulation mechanisms in post-quantum cryptography were applied to hardware accelerators for: Frodo KEM, Sabre, and NTRU, which have qualified for the round 3 PQC standardisation process by NIST. Their findings revealed acceptable overhead and high error coverage for all three studied NIST PQC. Augmenting the security of cryptographic algorithms by protecting them against side-channel active attacks (and natural faults) is essential in cryptographic engineering (Kermani, Bayat-Sarmadi, Ackie, & Azarderakhsh, 2019). The BLAKE algorithm is introduced as an efficient hash function developed based on Bernstein's ChaCha stream cypher. On the flip side, attacks are critical when implementing security and privacy usage models in PQC. In this post-quantum age, code-based cryptography is one feasible solution whose hardware architectures have become the research focus in the NIST standardisation process (Canto, Kermani, & Azarderakhsh, 2022). They work on efficient fault detection schemes based on regular parity, interleaved parity, and two cyclic redundancy checks (CRCs), i.e., CRC-2 and CRC-8. They performed error detection capability assessments and implementations on the field-programmable gate array Kintex-7 device xc7k70tfbv676-1 to verify the practicality of the presented approaches. Code-based cryptosystems could make use of these schemes.

Literature Review

In the contemporary competitive landscape, businesses are placing cybersecurity at the forefront of their priorities as they navigate the transition to a digital economy. Among the significant challenges in ensuring cybersecurity in the digital workplace, the human factor, particularly the actions of employees, stands out as a major obstacle. Virtual experience among workers and remote working are among the benefits of a digital workplace (Colbert, Yee, & George, 2016). On a global scale, the challenges of employees faced related to cybersecurity have been recognized as a critical issue in the digital workplace, underscoring the fact that the digitisation has become the new standard for businesses. This transition led to new cybersecurity challenges (Anant et al., 2020). Employees are more prone to vulnerability in respect of cybersecurity defence of any organization, endangering the organization by falling victim of social engineering attacks or usage of weak passwords (Chapman, 2021). According to Dell Technologies, 72 percent of employees are willing to exchange confidential information for money (Rantanen, 2021). Result showed that 64 percent of workers shy away from data sharing security, which pose a significant issue. However, another challenge is the usage of personal devices for work-related tasks. Many employees use personal devices to access work-related information.

Available data on Zippia shows that 83 percent of companies allow employees to use their own devices for company tasks (Zippia, 2022). The results indicated that 95 percent of employers adopted ‘bring your own device’ (BYOD) due to technological advancements and perceived costs of providing secured devices for workers, and that 57 percent of employees prefer the convenience of keeping track of personal and work-related items on a single device (Samsung). Therefore, it is no surprise that the global BYOD market size is expected to grow by US$69.07 billion from 2021 to 2026 (Technavio, 2022). Research by Bitglass revealed that 82 percent of companies allow employees to work using their personal devices (Palanisamy, Norman, & Mat Kiah, 2021). Personal devices may not possess adequate level of security measures as company provided devices and can lead to security breaches. In contrast, results showed that 90 percent of data breach occur as a result of human error (Barta, 2018). The research revealed risk and vulnerabilities associated with online activities not known by employees which leads to personnel engagement and put organizations at risk. Also, Stock *et al.* (2018) discovered that employees were common targets of cyberattacks, with cybercriminals using tactics like phishing and social engineering that exploited the human factor. Many employees were unaware of the associated dangers, making them vulnerable targets.

Ogunyemi & Idowu (2023) concluded that COVID-19 pandemic increased the adoption of business digitization in Nigeria, and cyberattacks is on the rise with remote working. The research revealed an increase in data breach which resulted by employees accessing organization information via unsecure network and personal devices. According to Ayodele (2022), 68 percent of businesses cited workers as their greatest cybersecurity loophole while 60 percent reported that their employees are their primary data source. Argaw *et al.* (2020) finding reveals 53 percent execute work related task with their own devices. 62 percent engage in work-related activities using public networks, representing a noteworthy cybersecurity risk. 46 percent of employees lack training on cybersecurity from their employers while 45 percent were unaware of their companies' cybersecurity policies (Piplai et al., 2020). This research offers insights into the specific cybersecurity challenges encountered by employees in Nigeria's digital landscape and lays a foundation for future regional cybersecurity research endeavours. However, Nigeria’s workplace is experiencing significant growth in digitization. There is few literatures on the cyber security hurdles encountered by Nigeria digital workplace. This gap underscores the need for further research to comprehend the cyber security challenges encountered by Nigerian digital workplace employees. The Cyber Security Expert Association of Nigeria (CSEAN) reports that there was an 87% surge in phishing attempts targeting SMEs in 2022, as opposed to a 37% increase in 2021. According to another report, there was an 89% surge in cyberattacks targeting Nigerian small and medium-sized enterprises (SMEs) in 2022. Consequently, limited previous studies on cybersecurity challenges in the Nigerian digital workplace have led businesses to express heightened concern about the need for research to understand the difficulties faced by employees in the region.

Research Methodology

This research aims at exploring and understanding the cybersecurity obstacles faced by employees in the Nigerian digital workplace. This investigation focused on identifying major obstacles and its impact on digitization of business in Nigeria. To achieve this goal, qualitative research methods, well-suited for exploring and understanding complex phenomena were employed. In-depth information were gathered qualitatively from participants, it gave insights and facilitate a comprehensive understanding of the research topic (Tracy, 2019). In this study, the primary data collection method employed was semi-structured interviews. It is chosen because of its suitability for garnering in-depth insights, flexibility, and exploration of the research topic. Semi-structured interviews were conducted with employees having experience in digital working environments across various enterprises in Nigeria. The interview guide consists of indefinite queries created to extract detailed responses from participants.

Interview Methodology

The interviews took place in a controlled environment conducive to open conversation, ensuring privacy and comfort for participants. The setting was a one-to-one, closed-door interview that ensured a neutral and professional atmosphere. At first, an appointment is agreed upon between the interviewer (researcher) and the prospective interviewee so as to gain the utmost trust and credibility of the participant for the purpose of the research. Each interview session lasted approximately 45 minutes to an hour, allowing ample time for participants to express their thoughts and experiences fully. Semi-structured format of interviewing with open-ended questions was employed to explore various aspects of the subject matter while also allowing for spontaneous discussion and follow-up inquiries. Prior to commencing the interviews, participants were provided with detailed information about the research objectives, procedures, and potential risks and benefits. Duly signed informed consent form was obtained from each participant, to ensure their voluntary participation and understanding of their rights within the study. Participants were assured of confidentiality and privacy, and measures were implemented to safeguard their anonymity in reporting and analysis.

Participant Selection

Participants were selected using a purposive sampling method based on candidates' experiences related to cybersecurity in the Nigerian digital workplace, characteristics, and attitude toward the task to ensure relevance and diversity within the sample. The selection criteria included individuals with direct experience in digital operations within Nigeria and demonstrated their expertise in cybersecurity. Efforts were made to recruit participants from various demographic backgrounds, professional fields, and levels of experience to enhance the representativeness of the sample.

To achieve diversity, outreach efforts were conducted through professional networks, academic institutions, and relevant organizations. Additionally, snowball sampling techniques were employed, wherein initial participants were asked to refer potential candidates who met the study's criteria, while the purposive technique was further used based on the referred candidates.

Data Saturation and Theme Development

Data saturation, the point at which no new data emerge from the interviews, was monitored throughout the data collection process. This was achieved by systematically analyzing interview transcripts and assessing for redundancy and saturation of themes.

To ensure the robustness of the developed themes, multiple strategies were employed:

a) **Constant Comparative Analysis:** Data analysis was conducted concurrently with data collection, allowing for the iterative refinement of themes and ensuring that emerging patterns were thoroughly explored.

b) **Peer Debriefing:** Regular discussions and debriefing sessions were held with peers and research colleagues to validate interpretations and ensure consensus on identified themes.

c) **Member Checking:** Preliminary findings and themes were shared with participants for validation, allowing them to provide feedback and confirm the accuracy of the interpretations.

The decision regarding data saturation and the robustness of themes was reached through consensus among the research team, taking into account the depth and breadth of the data as well as the coherence and consistency of the identified themes across different participants and contexts.

Thematic qualitative analysis

Below are the discussions on different themes that were identified from the data collected from employees of a digital workplace in Nigeria. The themes are presented as shown in Table 1 in the following manner:

First, familiarization with participant responses on the topic was conducted to extract initial ideas from each participant. Interesting ideas were assigned codes to group related ideas together. These codes were then used to identify potential themes. The potential themes were further assessed to ensure that each code correlated with the respective theme. Finally, the themes were refined, finalized, and named.

Table 1: Themes and Codes for Cyber Security Hurdles among Employees in the Digital Workplace in Nigeria

SN	Themes	Codes	No. of Respondent
1	Inadequate Awareness and Lack of Training	 Lack of Cyber Training </br> Awareness of Cyber Security Risks </br> Insufficient Cyber Hygiene Training</br>	6
2	Weak Passwords and Authentication	 Weak Passwords </br> Similar Passwords </br> Poor Authentication Methods </br>	6
3	Bring Your Own Device (BYOD)	 Risk associated with BYOD </br> Lack of Policies and Procedures for BYOD </br> Poor Security Practices on Personal Devices </br>	5
4	Insider Threats	 Malicious Insider Activities </br> Accidental Insider Activities </br> Sensitive Information Shared by Employees </br>	3
5	Social Engineering Attacks	 Phishing Attacks </br> Spear Phishing Attacks </br> Pretexting Attacks </br>	7
6	Remote Work	 Increase Risks of Cyber Threats </br> Lack of Awareness of Remote Work Cyber Risks </br> Inadequate Security Measures for Remote Work </br>	3

Source: Author's Findings

Inadequate Awareness and Lack of Training

Deficiency in cybersecurity awareness and training within the digital working environment was identified by the first theme. Employees expressed concerns about insufficient knowledge regarding potential cyber threats and a perceived inadequacy in training programs provided by their respective organizations. This can lead to employee's engagement in behaviour that jeopardizes organization's security. Quotations from six interviewees is represented in Table 2.

Table 2: Participant Response Under Lack and Inadequate Awareness and Training

Interviewee	Nature of Organization	Years of Experience	Current Role	Response
2	Finance	14	Head of Operations	"Discovered that our staff commonly exhibited low awareness of cybersecurity risks and the need to address it urgently".
7	Education/ Higher Institution	20	Director of ICT/ Senior Lecturer	"Found that our staff exhibited low awareness of cybersecurity risks, necessitating urgent intervention."
12	eCommerce	10	Marketing Manager	"We noticed many of our staff lacked awareness of basic cybersecurity practices, posing a significant concern for the organization."
4	Fintech	12	DevOps Engineer	"We realized that lack of cyber security training among our workers is a major vulnerable concern for our company."
15	Fintech	7	Information Security Analyst	"Lack of cyber security training exposed the organization to malware and phishing threats."
28	Technology	14	Senior Software Engineer	"Negligence of junior developer to cyber security training put our organization in a position vulnerable to cyber threats."

Weak Passwords and Authentication

The second theme revolves around "Weak Passwords and Authentication," emphasizing the risks associated with insufficient password strength and authentication methods. This includes concerns about password reuse and the utilization of easily guessable passwords. Such practices heighten the vulnerability of sensitive information and systems, providing attackers with an easier path to unauthorized access. Table 3 shows the quotations from respondents that shed light on their experiences and perspectives related to the challenges posed by weak passwords and authentication methods.

Table 3: Participant Response Under Weak Passwords and Authentication

Interviewee	**Nature of Organization**	**Years of Experience**	**Current Role**	**Response**
5	eCommerce	7	Web Developer	"Using same passwords across accounts can have serious consequences, especially if one account is compromised."
10	Finance	20+	Chief Technology Officer	"Usage of weak passwords provide cyber criminals with easy unauthorized access to our systems and data."
13	Finance	5	IT Support Officer	"Inadequate authentication methods, like SMS code verification and security questions can be easily bypassed by attackers."
19	eCommerce	8	IT Support Officer	"The number of times I've seen colleagues using '123456' as their password for sensitive company accounts is alarming."
22	Technology	11	Senior Developer	"People tend to choose convenience over security, which puts us all at risk. Stricter password policies needed to be applied."
24	Education	5	System Analyst	"Reusing passwords across multiple accounts poses serious risks, particularly if one account is compromised."

Bring Your Own Device (BYOD)

The third theme underscores the challenges associated with workers using own devices for work. This encompasses risks such as the potential loss or theft of devices. The interview quotations from five different interviewees provide insights into the varied experiences and perspectives regarding the challenges posed by this theme in the workplace, as represented in Table 4.

Table 4: Participant Response Under BYOD

Interviewee	Nature of Organization	Years of Experience	Current Role	Response
1	Education	10	Coordinator ICT	“Employees may unintentionally expose the organization to cyber threats when clear policies are procedures are lacking.”
9	Technology	17	Operation Manager	“Instances have arisen where staff exhibited poor security practices such as password sharing and untrusted download from the internet.”
17	Technology	8	Full stack Developer	“Allowing employees to use personal devices for work purposes can introduce several risks, like unsecured Wi-Fi networks or unapproved apps.”
26	Fintech	10	Information security Analyst	“Bring your own device blurs the line between personal and work devices. Most employees don't understand the importance of keeping work-related data secure on their personal phones.”
27	eCommerce	5	IT Support Staff	“I appreciate the flexibility of BYOD, but without proper guidelines, employees may inadvertently expose confidential information. We need clearer policies.”

Insider Threats

The fourth identified theme revolves around "insider threats." This theme delves into risks associated with employees engaging in activities that intentionally or unintentionally compromise security. It encompasses both malicious and accidental insider activities, as well as instances of employees sharing sensitive information. The recognition of these insider threats underscores the potential for data breaches and other cybersecurity incidents within the organization. Responses from participants are shown in Table 5, which provide insights into the experiences and challenges associated with this challenge.

Table 5: Participant Response Under Insider Threats

Interviewee	**Nature of Organization**	**Years of Experience**	**Current Role**	**Response**
6	Finance	22	Head of Operations	"We found that certain employees share sensitive information with unauthorized parties, posing a significant risk to our organization."
18	Education	17	Confidential Secretary	"A major data breach occurred due to malicious insider activities, serving as a wake-up call for our department."
29	Finance	4	Bank Teller	"Accidental actions such as clicking on malicious links or downloads from untrusted sources pose severe consequences for the organization."

Social Engineering Attacks

The fifth theme centers on "Social Engineering Attacks." This theme underscores the prevalence of social engineering attacks encountered by employees, such as phishing and pretexting attacks. These deceptive tactics aim to deceive employees to undertake actions that jeopardize the organization's security. Quotations from respondents provide insights into the experiences and challenges associated with this theme and is represented in Table 6.

Table 6: Participant Response Under Social Engineering Attacks

Interviewee	**Nature of Organization**	**Years of Experience**	**Current Role**	**Response**
3	Finance	15	Head of Operations	"Phishing incidents are becoming more sophisticated, and it's imperative that our employees receive training to recognize and avoid them."
8	eCommerce	9	IT Manager	"Pretexting attacks commonly involve impersonating trusted

				sources and can be mis-leading if not vigilant.”
16	Finance	3	Bank Teller	“During a simulated phishing exercise, many of us were fooled by fake emails pretending to be from company executives. It showed us how easily we can be manipulated.”
18	Governmental/ Education	28	Bursar	“Heard of improvement in social engineering attacks which target employees through phone calls and text messages.”
20	Finance	6	Customer Service Officer	“I received an email that looked exactly like it was from our IT department, asking me to update my password. I almost fell for it until I noticed the email address was slightly different.”
25	Technology	11	Network Administrator	“Spear phishing attacks are very sophisticated so that they focus on specific individuals or groups and are challenging to identify.”
30	Education	15	Senior Lecturer/ Head of Department	“After fallen a victim of a pretext email posing to be from a colleague, I'm more cautious about emails, even from people I know.”

Remote Work

The sixth theme revolves around "Remote Work," focusing on associated cybersecurity threats. It encompasses lack of awareness regarding the risks associated with remote work and insufficient measures to mitigate these risks. The interview quotations from three different interviewees provide valuable perspectives and experiences related to the challenges posed by remote work in terms of cybersecurity. Participant responses are represented in Table 7.

Table 7: Participant Response Under Remote Work

Interviewee	Nature of Organization	Years of Experience	Current Role	Response
14	Technology	8	Software Engineer	"Many employees lack awareness of cyber risks linked with remote work, such as phishing emails that mimic communication from their employer."
16	Technology	3	Junior Full Stack Developer	"Embracing remote work with unsecure infrastructure exposed our organization to novel cyber threats."
20	Technology	7	UI/UX Engineer	"Employees often use unsecured public Wi-Fi networks while working remotely, making them vulnerable to cyber-attacks. It's crucial to educate staff about the risks and provide secure remote access solutions."

Discussion

The study aimed to investigate challenges faced by personnel within the Nigerian digital organization as related to cyber security. Data were gathered by semi-structured interviews while qualitative approach was employed. Six themes were generated, first is lack of awareness and inadequate training. This underscored the notable challenge posed by employees' insufficient attention and training in the realm of technology within the digital workplace. Williams *et al.* (2019) and Alqahtani (2021) findings revealed that training and awareness of employees on cyber security represent a significant challenge in the digital workplace, resulting in workers ignorantly clicking on suspicious links or downloading malicious attachments from untrusted source, making organization's data and systems vulnerable to attacks. Consequently, there is a crucial need for businesses to offer comprehensive and continual cybersecurity training to their employees. The second theme identified was "weak passwords and authentication", signifying significant challenges in the digital workplace stemming from poor passwords and insufficient authentication systems prone to exploitation by cybercriminals (Johnson, 2016). Instances such as employees using identical passwords across multiple accounts or employing easily guessed passwords contribute to these issues. To mitigate the risks associated, organizations should enact strict policies and procedures. Among the possible policies is to mandate multiple forms of authentication and robust password practices such as inclusion of uppercase, lowercase, numbers, and symbols before a password could be accepted.

Next on the list is BYOD, which highlights the growing acceptance of employees using personal devices to work. This practice is associated with risks such as malware infections, potential device damage, and unauthorized access to organisation data (Aigbefo, 2022). Organizations are actively working to mitigate the threats posed by these practices. This can be achieved by organizations procuring enough sophisticated systems to be used by members of staff for office work.

The fourth theme, "Insider Threat," emerges as a major concern in the digital workplace. This involves employees potentially engaging in activities, whether intentional or unintentional, that compromise the organization's cybersecurity (Alotaibi & Alshehri, 2020). Examples include disclosure of sensitive information or inadvertently downloading malware onto their devices. To mitigate the likelihood of insider threats, businesses are advised to educate employees about the consequences associated with such threats and implement stringent access controls and assessment mechanisms. To mitigate this threat, organizations need to create a different level of access to the company's resources, where experienced senior staff are saddled with more responsibility and could only access sensitive organization information.

Also, cybercriminals frequently employ “social engineering attacks,” which is the fifth theme for this research, including phishing, spear phishing, and pretexting, as tactics to gain access to sensitive data and platforms (Grimes 2021). These attacks often take advantage of employees' limited awareness and training, tricking them into revealing login credentials or downloading malware. Organizations can mitigate the risks associated with social engineering attacks by educating employees about different attack types and implementing technical safeguards, such as anti-phishing software and email filtering. On the flip side, working remotely poses a negligence challenge to standard digital work settings as compared to freelancing. Employees working remotely are not fully monitored, which exposes the organization to serious risks when connected to unsecure networks. Also, there are higher chances of an employee using a personal device for office work when working remotely.

The fig. 1 below is the theoretical model of the challenges faced by employee and its implication whether managed or not on the digital organization.

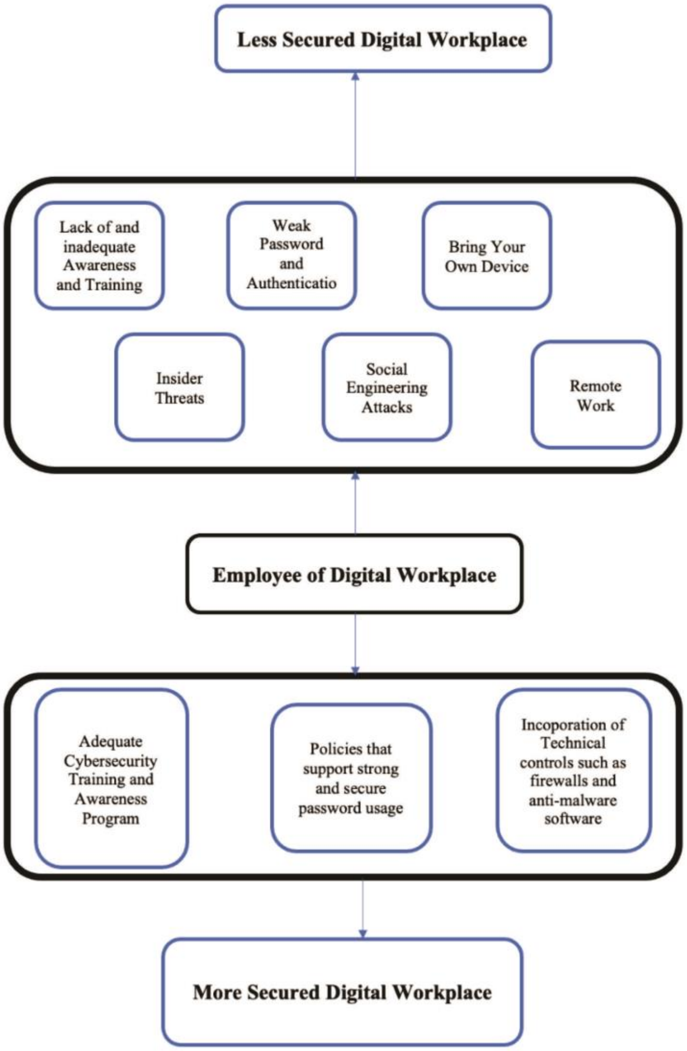
Less Secured Digital Workplace
Lack of and inadequate Awareness and Training
Weak Password and Authenticatio
Bring Your Own Device
Insider Threats
Social Engineering Attacks
Remote Work
Employee of Digital Workplace
Adequate Cybersecurity Training and Awareness Program
Policies that support strong and secure password usage
Incoporation of Technical controls such as firewalls and anti-malware software
More Secured Digital Workplace

Fig 1: Theoretical Model

Theoretical and Practical Implications

The outcome of the study holds both theoretical and practical implications, with a focus on cyber security and digital workplace management. Theoretical implications are discussed below, highlighting the importance of cyber security as related to employee behaviour and attitudes. The identified themes advocate for a proactive rather than reactive approach to cyber security, particularly in dealing with BYOD, social engineering attacks, and remote work scenarios, where personnel may inadvertently expose the organization to cyber risks. Furthermore, lack of and inadequate awareness and training, weak password and authentication, and insider threats underscore the significance of addressing employee behaviour and awareness to mitigate cyber security risks.

Beyond theoretical implications, the study holds practical significance for organizations operating in the digital workplace in Nigeria. The findings underscore the imperative for firms to prioritize employee cybersecurity training through frequent programs aimed at enhancing awareness of cybersecurity issues and fostering good cyber hygiene practices. These trainings would keep the staff updated on the latest trends in cybercrime and cybersecurity, thereby mitigating the threats the organization is exposed to as a result of the negligence of the employee. On the flip side, the research suggests the implementation of robust methods of authentication and policies to reduce risks associated with insecure passwords. Among the possible policies that could be employed by organizations is the inclusion of uppercase, lowercase, numbers, and symbols before a password could be accepted. Also, there are mechanisms for the automatic generation of passwords for company accounts that could be implemented into organization software; these passwords are difficult to get.

The need for comprehensive BYOD policies and procedures, including the incorporation of security controls such as firewalls and anti-malware software is emphasized. Additionally, in line with working remotely, businesses are encouraged to put in place measures to safeguard remote work environment. Concrete measures, such as utilizing secure remote access technologies, implementing multi-factor authentication, and incorporating data encryption, are recommended to reduce the vulnerabilities associated with remote work.

The practical implications underscore the importance of adopting a proactive approach to cybersecurity which involves prioritizing employee training and awareness, implementing strong policies, and employing technical controls to mitigate risks associated with cybersecurity hurdles in Nigeria's digital workplace. Overall, the study advocates for a comprehensive and pre-emptive strategy to address the evolving landscape of cybersecurity in the Nigerian digital workplace.

Conclusion

In conclusion, this study sheds light on the cybersecurity challenges faced by Nigerian employees in the digital workplace. Through a cross-sectional analysis, we have identified several key factors influencing employees' cybersecurity practices, including awareness, training, organizational policies, and technology infrastructure. The findings underscore the importance of addressing these factors to enhance cybersecurity resilience and protect against emerging threats in the Nigerian context.

References

Aigbefo, Q. A. (2022). Understanding SME employees' security behaviours when performing work tasks using BYOD from multiple work locations (Doctoral dissertation, Macquarie University).

Ajufo, G., & Qutieshat, A. (2023). An Examination of the Human Factors in Cybersecurity: Future Direction for Nigerian Banks. *Indonesian Journal of Information Systems*, *6*(1), 1-16. https://doi.org/10.24002/ijis.v6i1.7278

Al Nafea, R., & Almaiah, M. A. (2021). Cyber security threats in cloud: Literature review. *In 2021 International Conference on Information Technology (ICIT)* (pp. 779-786). IEEE. https://doi.org/10.1109/ICIT52682.2021.9491638

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2), 23. https://doi.org/10.3390/bdcc5020023

Alotaibi, F., & Alshehri, A. (2020). Gender differences in information security management. *Journal of Computer and Communications*, 8(3), 53-60.

https://doi.org/10.4236/jcc.2020.83006

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. Applied Sciences, 12(5), 2589. https://doi.org/10.3390/app12052589

Alrubaiq, A., & Alharbi, T. (2021). Developing a cybersecurity framework for e-government project in the Kingdom of Saudi Arabia. *Journal of Cybersecurity and Privacy*, 1(2), 302-318. https://doi.org/10.3390/jcp1020017

Anant, V., Banerjee, S., Li, K., & Boehm, J. (2020). A dual cybersecurity mindset for the next normal. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-dual-cybersecurity-mindset-for-the-next-normal

Anastasova, M., Azarderakhsh, R., & Kermani, M. M. (2022, August). Time-optimal design of finite field arithmetic for sike on cortex-m4. In International Conference on Information Security Applications (pp. 265-276). Cham: Springer Nature Switzerland.

Apostolopoulos, T., Katos, V., Choo, K.-K. R., & Patsakis, C. (2021). Resurrecting anti-virtualization and anti-debugging: Unhooking your hooks. Future Generation Computer Systems, 116, 393-405. https://doi.org/10.1016/j.future.2020.11.004

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., & Eshaya-Chauvin, B. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC medical informatics and decision making, 20, 1-10. https://doi.org/10.1186/s12911-020-01161-7

Ayodele, C. (2022). Mitigating cybersecurity insider threat in the hiring stage of the employee lifecycle. Preprint from PsyArXiv. https://doi.org/10.31234/osf.io/cmeur

Back, S., & Guerette, R. T. (2021). Cyber place management and crime prevention: the effectiveness of cybersecurity awareness training against phishing attacks. *Journal of contemporary criminal justice*, 37(3), 427-451. https://doi.org/10.1177/10439862211001628

Barta, G. (2018). The increasing role of IT auditors in financial audit: risks and intelligent answers. Business, Management and Education, 16(1), 81-93. https://doi.org/10.3846/bme.2018.2142

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Butt, U. A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M. T., & Albaqami, N. (2023). Cloud security threats and solutions: A survey. Wireless Personal Communications, 128(1), 387-413. https://doi.org/10.1007/s11277-022-09960-z

Canto, A. C., Kermani, M. M., & Azarderakhsh, R. (2022). Reliable constructions for the key generator of code-based post-quantum cryptosystems on FPGA. ACM Journal on Emerging Technologies in Computing Systems, 19(1), 1-20.

Canto, A. C., Sarker, A., Kaur, J., Kermani, M. M., & Azarderakhsh, R. (2022). Error detection schemes assessed on FPGA for multipliers in lattice-based key encapsulation mechanisms in post-quantum cryptography. IEEE Transactions on Emerging Topics in Computing, 11(3), 791-797.

Chapman, P. (2021). Defending against insider threats with network security's eighth layer. Computer Fraud & Security, 2021(3), 8-13. https://doi.org/10.1016/S1361-3723(21)00029-4

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. IEEE Access, 10, 85701-85719. https://doi.org/10.1109/ACCESS.2022.3197899

Colbert, A., Yee, N., & George, G. (2016). The digital workforce and the workplace of the future. *Academy of Management Journal*, 59(3), 731-739. https://doi.org/10.5465/amj.2016.4003

Gazzan, M., Alqahtani, A., & Sheldon, F. T. (2021). Key Factors Influencing the Rise of Current Ransomware Attacks on Industrial Control Systems. *In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference* (CCWC) (pp. 1417-1422). IEEE. https://doi.org/10.1109/CCWC51732.2021.9376179

Grimes, R. A. (2021). Social engineering attacks.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. Field methods, 18(1), 59-82. https://doi.org/10.1177/1525822X05279903

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, 45, 3171-3189. https://doi.org/10.1007/s13369-019-04319-2

Ilves, L. K., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. (2016). European union and nato global cybersecurity challenges. Prism, 6(2), 126-141. https://www.jstor.org/stable/26470452

Johnson, M. (2016). Cybercrime, security and digital intelligence. Routledge. https://www.perlego.com/book/1570296/cyber-crime-security-and-digital-intelligence-pdf

Kermani, M. M., Bayat-Sarmadi, S., Ackie, A. B., & Azarderakhsh, R. (2019, February). High-performance fault diagnosis schemes for efficient hash algorithm blake. In 2019 IEEE 10th Latin American Symposium on Circuits & Systems (LASCAS) (pp. 201-204). IEEE.

Ogunyemi, R., & Idowu, A. (2023). Data Security Concerns Raised by ‘Bring Your Own Device’ in Corporate Organisations’ Hybrid and Remote Work Environments in Nigeria. *The Commonwealth Cybercrime Journal*, 111.

Oloidi, A. (2019). Cyber-security Challenges in Financial Institutions in Nigeria: A Multiple Case Study (Doctoral dissertation, Northcentral University).

Palanisamy, R., Norman, A. A., & Mat Kiah, L. (2021). BYOD security risks and mitigation strategies: Insights from IT security experts. *Journal of Organizational Computing and Electronic Commerce*, 31(4), 320-342. https://doi.org/10.1080/10919392.2022.2028530

Piplai, A., Mittal, S., Joshi, A., Finin, T., Holt, J., & Zak, R. (2020). Creating cybersecurity knowledge graphs from malware after action reports. IEEE Access, 8, 211691-211703. https://doi.org/10.1109/ACCESS.2020.3039234

Rantanen, O. (2021). Security Criteria Awareness (Master’s Thesis, Jyväskylä: JAMK University of

Applied Sciences). https://urn.fi/URN:NBN:fi:amk-2021060113103

Ruslin, R., Mashuri, S., Rasak, M. S. A., Alhabsyi, F., & Syam, H. (2022). Semi-structured Interview: A methodological reflection on the development of a qualitative research instrument in educational studies. IOSR *Journal of Research & Method in Education* (IOSR-JRME), 12(1), 22-29.

Safavi, K., & Kalis, B. (2019). Accenture 2019 Digital Health Consumer Survey. Accenture. https://www.ehidc.org/sites/default/files/resources/files/Accenture-2019-Digital-Health-Consumer-Survey.pdf

Samsung (no date), 'Maximizing Mobile Value', White Paper, Samsung Business, available at: www.samsung.com/us/business/short-form/maximizing-mobile-value-2022

Savić, D. (2020). COVID-19 and work from home: Digital transformation of the workforce. Grey Journal (TGJ), 16(2), 101-104. https://dobrica.savic.ca/pubs/TGJ_V16_N2_Summer_2020_DS_article.pdf

Stock, T., Obenaus, M., Kunz, S., & Kohl, H. (2018). Industry 4.0 as enabler for a sustainable development: A qualitative assessment of its ecological and social potential. Process Safety and Environmental Protection, 118, 254-267. https://doi.org/10.1016/j.psep.2018.06.026

Technavio (2022), 'Bring your own Device (BYOD) Market by End-user and Geography – Forecast and Analysis 2022–2026', Technavio.com. September, available at: https://www.technavio.com/talk-to-us?report=IRTNTR74271&type=sample&rfs=epd&src=report&utm_source=prnewswire&utm_medium=pressrelease+&utm_campaign=t42dtcs_rfs1_wk41_2022_007&utm_content=IRTNTR74271

Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. (2017). Cyber security threats to IoT applications and service domains. Wireless Personal Communications, 95, 169-185. https://doi.org/10.1007/s11277-017-4434-6

Williams, A. S., Maharaj, M. S., & Ojo, A. I. (2019). Employee behavioural factors and information security standard compliance in Nigeria banks. *International Journal of Computing and Digital Systems*, *8*(04), 387-396.

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. European journal of education, 48(2), 311-325. https://doi.org/10.1111/ejed.12014

Zippia (2022), '26 surprising BYOD statistics [2022]: BYOD trends in the workplace', Zippia.com, 17 October, available at: https://www.zippia.com/advice/byod-statistics/ (accessed 7 April 2023).