An Examination of the Human Factors in Cybersecurity: Future Direction for Nigerian Banks

G K Ajufo[*1], A Qutieshat[2]

[1]Directorate of Research and Graduate Studies, University of Zambia

[2]University of Dundee, Dundee, Scotland, United Kingdom

E-mail: gkajufo@gmail.com*[1], aqutieshat@dundee.ac.uk [2]

Submitted: 6 May 2023, revised: 14 July 2023, accepted: 28 July 2023

Abstract. Information and communication technology has become necessary for conducting business operations and ensuring business survival in Nigerian banks. However, this has come with some encumbrances, as this technology is vulnerable to attacks due to technical or human factors. These human factors have been very challenging for organizations due to their multi-dimensional nature and the fact that humans have been responsible for most cybersecurity incidents. Resolving issues arising from cybersecurity incidents is expensive and time-consuming. Therefore, this study is crucial as it will enable Nigerian banks witnessing increased attacks to take preventive measures and reduce the enormous expenditure required for remediation. This study adopts a literature review approach, reviewing previous studies on human factors in cybersecurity to determine the factors responsible for successful cyber-attacks and their suggested mitigations. The findings categorize these human factors into social engineering, poor information security culture, risky password practices, stress, burnout, and security fatigue. The study presents mitigations but notes that training and cybersecurity awareness are the most common reoccurring pre-emptive actions recommended. This research is significant as very little prior research has been conducted in this area targeted at the Nigerian banking sector. Practically, the findings of this study are expected to point Nigerian banks toward the critical human factors that they need to concentrate on to minimize the success rate of cyber-attacks and reduce the associated costs of recovering from these attacks.

Keywords: human factor, cybersecurity, social engineering, phising, information security culture.

1. Introduction

Information and communication technology (ICT) has become ubiquitous and necessary for business operations and survival in our competitive global environment. The Nigerian banking sector is not an exception, as ICT has significantly improved service efficiency, worker performance, and profitability by deploying automated teller machines and online banking applications [1]. ICT has also facilitated increased returns on equity for deposit money banks (DMBs) and should therefore be integral to banks' strategies as it is envisaged to drive increased profitability, efficiency, and competitiveness [2].

However, despite the many advantages of ICT, vulnerabilities exist, which can result in dire consequences for organizations when exploited. A case in point is the WannaCry ransomware attack of

May 2017, which encrypted user files on computers running Microsoft Windows in at least 150 countries, blocking access to such files until a ransom was paid in the form of bitcoin, and has been described as causing one of the worst cyber-attacks ever witnessed [3, 4, 5].

While cybersecurity vulnerabilities may be due to technical issues, research has shown that human factors also strongly influence cyber-attacks, as humans usually constitute the weakest link in the cybersecurity protection chain [6, 7, 8] and are the cause of the majority of many information security breaches in organizations due to their poor cyber security hygiene [9, 10, 11]. This position is supported by [12], who contend that the larger the number of people in an organization, the greater the likelihood of a breach in information security, as it only takes a mistake by one individual to compromise an organization's entire network.

Remediating breaches arising from human factors could require substantial annual costs of between $4.1 and $6.6 million, as reported by the Ponemon Institute, the foremost organization dedicated to research on privacy, data protection, and policy on information security [13]. In Nigeria, a report issued by the Nigeria Interbank Settlement System (NIBSS), the organization responsible for coordinating clearing and interbank payments in Nigeria, indicates that fraud cases have increased by 186% from 2019 to 2020, with social engineering accounting for 56% of these attempts [14]. The NIBSS report also indicates that fraud attempts via mobile channels increased by 330% during the same period, while cases of fraud via the web increased by 173%, with over 91% successful attempts.

Given these issues and the attendant cost to banks, this study seeks to determine the human issues of organizational insiders that lead to the success of cybersecurity attacks in Nigerian banks and offer mitigating actions that will minimize the associated costs of cybersecurity incident recovery.

This study is critical because although several studies have been conducted globally on the importance of the human factor in cyberattacks, to the best of our knowledge, very little research targeted at the Nigerian banking sector in this area has been carried out before this research. Furthermore, this study is significant as it is the first study to the best of our knowledge to provide solutions to the issue of human factors in cybersecurity in Nigerian banks by combining findings from global research and the results of studies on cybercrime and cybersecurity in Nigerian banks.

2. Cybersecurity and The Human Factor

Cybersecurity has been defined in several ways. The ISO/IEC 27032:2012 standard defines cybersecurity as "the preservation of confidentiality, integrity, and availability of information in cyberspace" [15]. The same standard also defines cyberspace as a "complex environment resulting from the interaction of people, software, and services on the Internet using technological devices and networks connected to it, which does not exist in any physical form." The US National Institute of Standards and Technology (NIST) offers many definitions, including that which defines cybersecurity as "the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" [16].

Technology is not self-driven, as humans must interact with it to achieve the desired results. Because of this, it is pertinent to understand the human behaviors and factors contributing to cybersecurity's success or failure. These behaviors refer to the choices people make to either mitigate cybersecurity issues using appropriate countermeasures or render information and communication technology systems insecure through actions that may be deliberate or from outside influence [17]. These human factors are multi-dimensional [18]. They may be unintentional due to a lack of knowledge or skills, intentional due to users knowingly engaging in risky behaviors that are in contravention of organizational policies and procedures and which may not result in any harm to the organization, or maybe malicious acts that are intentional and performed to bring harm to the organization [19].

Human factors are important and challenging for organizations, as humans have been responsible for most cybersecurity incidents [10]. Furthermore, Prabhu and Thompson [20] contend that human factors are the main motivating factors for insider attacks arising from personality traits, human emotions, financial needs, external loyalties, knowledge and skills, interconnectedness, and organizational culture. Therefore, understanding how human factors influence online behaviors and attitudes, especially in children, is critical as it will reinforce cybersecurity awareness and improve cyber hygiene [21]. Unfortunately, understanding human behavior is problematic because it is multi-dimensional and multi-faceted, making it difficult to quantify all human factors, which makes it impossible to apply a single solution to every situation [20].

3. Research Method

This study used the literature review approach sourcing its materials from the Web of Science and Google Scholar databases which provide publication data and other information such as references and article citation indexes. The focus of the research was clearly outlined: to ascertain the human-centric factors within organizations contributing to the success of cybersecurity attacks, with an emphasis on Nigerian banking institutions. The research further aimed to propose actionable mitigation strategies to minimize the financial burden of cybersecurity incident recovery.

The research process commenced with identifying suitable databases for sourcing literature and determining the criteria for inclusion and exclusion. A rigorous search ensued, with each piece of identified literature scrutinized for relevance to the overarching research objective. The extracted literature was meticulously synthesized, with the study's findings, conclusions, and recommendations documented systematically.

3.1. Inclusion and Exclusion Criteria

The target publications were peer-reviewed articles from the Web of Science and Google Scholar databases from 2013 to 2023 related to human factors in cybersecurity and cybersecurity in Nigerian banks. Thus, conference papers, books, book chapters, theses, and dissertations were omitted. Also, only articles written in the English language were considered. These criteria yielded an initial number of 65 articles from the Web of Science and 33,100 from the Google Scholar database, as it was impossible to exclude conference papers, books, book chapters, theses, and dissertations from the search on Google Scholar. After eliminating duplicates and checking for suitability, a further review of these articles yielded 43 Web of Science articles and 20 Google Scholar articles, giving 63 relevant articles published between 2014 and 2023 for the study. Table 1 shows the number of articles by year of publication.

Table 1. List of Articles by Year of Publication

Year of Publication	Number of Articles
2014	1
2015	3
2016	1
2017	3
2018	5
2019	6
2020	9
2021	13
2022	20
2023	2

4. Result

The extant literature reviewed revealed several human factors responsible for the successful exploits of cybersecurity vulnerabilities. These are categorized as social engineering; risky password practices; poor information security culture; stress, burnout, and security fatigue and are presented subsequently. Although very little research has been conducted on the issue of human factors in cybersecurity in Nigerian banks, some studies have been conducted on the issue of cybersecurity and cybercrime in Nigeria. Accordingly, a fifth section on Information Security in Nigeria highlights the rising cases of cyberattacks in Nigerian banks to show that the global trends in cybersecurity discussed under the four other categories equally apply to Nigerian banks.

4.1. Social Engineering

Social engineering attacks use deception to manipulate individuals into giving away confidential or personal information that can be used to perpetrate cyber-attacks and are major avenues for facilitating cyber-attacks [22, 23]. Social engineering is classified as an attentional vulnerability, as successful attacks such as those from outsiders or those resulting from users sending misdirected emails that expose confidential information are due to human inattention [24]. Attacks based on social engineering are obscure and do not follow any established approach, which makes them very effective, efficient, and relatively easier than undertaking attacks using technical means. They are popular because it is easier to trick humans into performing desired actions than discover technical vulnerabilities in systems, thus making them difficult to counter [25].

One of the vectors for social engineering attacks is phishing, which involves sending emails to potential victims while masking the source to indicate that they come from a trusted source to deceive victims into revealing confidential information such as passwords. Phishing is considered the most common social engineering attack vector. It can also be achieved via technical subterfuge, in which the attacker plants malicious code to steal confidential information when an attachment is opened [23, 26, 27, 28, 29]. Phishing attacks rely on deception like other social engineering attacks but can only succeed if the target responds [30]. Social engineering attacks include dumpster diving, where sensitive information that can be used for attacks is obtained from trash, and scareware, in which attackers use the human emotions of fear, anxiety, etc., to trick humans into installing malicious software [25].

Another type of social engineering attack is the "water hole" attack, in which the attacker finds a target organization and a site they frequently visit. After that, the attacker compromises this legitimate website and redirects visitors to another site where malicious activities are initiated. Once this compromise is achieved, the attacker may proceed to infect other systems on the network [25].

Additional social engineering attacks are reverse social engineering, where the attacker creates a problem for the target and then presents the target with a solution to the problem, enabling the attacker to gain trust, which is later used to obtain sensitive information to manipulate the target, and deepfake, which is a recent attack vector used to forge images, video, and audio to achieve the malicious intent of the attacker [25].

Social engineering attacks pose significant threats to the data and infrastructure of organizations as they can sometimes be difficult to detect even to the trained eye, especially when users are using mobile devices to access emails, which makes it difficult to hover over links to expose the true destination of the link [25]. This lack of detection may also be due to the prevalence effect, a phenomenon in which targets are not discovered due to their low occurrence frequency [31].

Desolda, Ferro, Marrella, Catarci, and Costabile [32] suggest that human factors such as lack of knowledge, resources, awareness, organizational norms, and complacency are key human vulnerabilities exploited by phishing cyber attackers. However, as Klimburg-Witjes and Wentland [32] noted, nobody is safe from these attacks, as even cybersecurity experts have been known to fall for social engineering attacks.

Addressing social engineering vulnerabilities requires changing user interfaces, addressing user attitudes and behaviors, educating users, introducing frameworks and models that improve user security [32], and instituting proper cybersecurity and communication policies [25]. Social engineering attacks can also be mitigated through proper training using delivery methods such as face-to-face, self-directed, and teachable moments [27] or using phishing simulations, which must be adequately planned to avoid an unnecessary increase in employee workloads that may be counterproductive [26, 28]. Awareness may also be improved by emphasizing the perceived threats from cyber-attacks, as this directly leads to increased human information-seeking behavior, while emphasizing the need to cope with social engineering may also indirectly improve the effectiveness of awareness campaigns [34]. Implementing anti-phishing protection guidelines can improve online interaction and thus improve organizational and individual cybersecurity postures [35].

4.2. Risky Password Practices

Globally, usernames and passwords are used as a prevalent means of authentication [36]. Due to the large number of websites users visit on an ongoing basis, these users are required to remember a significant number of passwords, a situation that results in cognitive overload and password fatigue, leading users to sometimes use default or weak passwords, reuse their passwords across sites, or recycle password patterns when the passwords expire [37, 38]. These insecure passwords have made passwords a significant contributor to successful breaches [39], as these passwords are susceptible to simple attacks such as dictionary attacks, thus making it easy for others to gain unauthorized access to confidential information [35]. Al-Slais and El-Medany [37] propose that adopting longer passwords or passphrases without necessarily enforcing password complexity may solve the problem of password fatigue. Alternatively, Alsharif, Mishra, and AlShehri [23] suggest using complex passwords with expiry dates and password histories as mitigating factors for weak and default passwords. Similarly, Neigel, Claypoole, Waldfogle, Acharya, and Hancock [40] recommend changing passwords routinely and avoiding recycling passwords as effective ways to tackle this issue.

4.3. Poor Information Security Culture

Georgiadou, Mouzakitis, Bounas, and Askounis [41] define information security culture at organizational and individual levels. At the organizational level, cultural elements affect organizational assets, continuity, access, trust, operations, defense, and security governance. The individual level contains elements like attitude, awareness, behavior, and competency. Poor information security culture has also been observed to affect the behavior of employees [42, 43]. This negative behavior may be due to inducement, manipulation, coercion, or insufficient knowledge and attitude toward security policies and procedures [43, 44, 45]. Fagan and Khan [46] and Philip, Luu, and Traci [47] also report that users' choices to abide by cybersecurity policies and procedures are made in line with the perceived risks of their actions in terms of minimizing costs and maximizing benefits. Wulandari, Adnan, and Wicaksono [48] concur, stating that increased cybersecurity risk perception, competence, and cyberattack experience reduce the susceptibility to cyberattacks.

Cyber threats may also result from unintentional insider actions when there is little or no attention to details, poor planning, and ignorance of cybersecurity even though there is no malicious or prior intent [48, 49] or insufficient capacity in terms of knowledge and skills [51, 52]. Similarly, insider threats may result from mistakes, negligence, greed, or recklessness [53, 54]. Khan, Houghton, and Sharples [55] submit that unintentional insider threats are due to decision-making, task factors, accidents, and organizational factors, where decision-making is influenced by lived experience and acquired knowledge, while task complexity, speed, and actions drive task factors. Other human behaviors, such as employees bypassing firewalls due to a lack of knowledge or to achieve specific intended purposes, may lead to successful cyber-attacks [56].

Several other actions include employees accessing harmful websites, using personal devices on company networks, sharing official information via social media, and using third-party removable media on organizational systems without scanning [56]. In another study, Szczepaniuk and Szczepaniuk [57] list human issues such as lack of ability to use security mechanisms, absence of cybersecurity training and education, risky actions taken consciously, and lack of awareness of the spread of malware as human factor vulnerabilities that can lead to successful cyber-attacks. In their study, Vrhovec, Bernik, and Markelj [34] suggest that human cybersecurity behaviors are influenced by whether people perceive that they receive social approval from important people by abiding by awareness campaigns (subjective norm), how negative or positive the individual perceives the awareness campaign to be (attitude towards behavior), how effective they perceive the efficacy of the awareness campaign (response efficacy), and how they perceive the overall performance of the state in dealing with errant behavior and social engineering (authorities performance). Similarly, Hadlington [38] posits that people who are extroverted, impulsive, less painstaking, and addicted to the internet are more likely to have risky behaviors toward cybersecurity. Likewise, cybersecurity incidents are affected by human cybersecurity behaviors, training, cybersecurity awareness, human error, lack of motivation, education, security self-efficacy, experience, skills, stress, and gender [10, 58].

Other human factors responsible for successful cyber-attacks related to user attitude, awareness, competency, and behavior are dissatisfaction from stressful life events, personality dispositions such as severe mental health disorders or personal issues, situational awareness, policies, and role awareness [59].

To improve user information security behaviors, organizations should employ people with personality traits such as openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism, satisfy employees, and conduct cybersecurity awareness and training [58]. Information security behaviors can also be improved by instituting and maintaining the required security culture by using the appropriate combination of rewards and punishments in line with the organization's culture, as it would positively influence employee behavior to comply with organizational security policies and procedures [42]. Elifoglu, Abel, and Tasseven [53] agree with this submission and advise that organizations should ensure employees are trained to detect suspicious activities and understand cybersecurity policies and penalties for violations. However, the severity of penalties may not influence information security policy compliance [60, 61]. Improving user information security behaviors can be achieved by conducting cybersecurity awareness campaigns, implementing meaningful non-intrusive security functions, and ensuring that security policies are available and easy to follow [10, 58].

Training activities that improve awareness can improve online interaction and thus improve organizational and individual cybersecurity postures [49, 51, 9, 35]. However, the one-size-fits-all approach to awareness is usually ineffective. Therefore, awareness campaigns must be personalized to everyone, as people have different responsibilities and levels of access and their own biases toward security [19, 34]. Mohammad, Hussin, and Husin [62], in their study on the application of the theory of human ecology to online safety awareness and human factors, argue that improving cybersecurity awareness requires that intra- and interpersonal factors that shape human behaviors be considered since the different layers of the social environment affect people’s behavior and well-being in different ways.

To assist users, companies should communicate the required behavioral attitudes toward deployed systems [44]. Pollini et al. [43] suggest the following measures to improve the security culture: Firstly, the content design of the information security program must consider the participants' perceptions of risk to mitigate against any perceived benefits they may think may accrue from their risky behaviors, while also ensuring that the content is proportionate to the participant's knowledge and skills. Secondly, work tools should be designed not to negatively affect the user experience while complying with security policies and procedures. Furthermore, security policies and procedures should not impede the realization of organizational goals, including safety and efficiency.

Practicing good cyber hygiene, such as ensuring that anti-virus software is up-to-date and constantly monitoring information technology infrastructure for vulnerabilities and threats, is another effective way of maintaining cybersecurity [40].

4.4. Stress, Burnout, and Security Fatigue

Cybercriminals have continuously succeeded in using human conditions such as stress, burnout, and security fatigue as vectors for security attacks, as organizations over time have adopted mainly technological solutions to solve these human problems [63, 19] rather than engaging human factors experts for advice on measures that will reduce or eradicate stress, burnout, and fatigue in the workplace [64]. Lahcen, Caulkins, Mohapatra, and Kumar [19] agree that stress and fatigue contribute to cybersecurity breaches, which may lead to unintentional damage, while loss of vigilance could lead to intentional damage. Chowdhury, Adam, and Skinner [65] and Blythe and Coventry [5] argue that users who are under pressure due to unresponsive IT support or the assignment of multiple tasks that are to be performed under tight deadlines can experience cognitive overload and stress, which can negatively impact their behavior and result in the compromise of cybersecurity measures. Similarly, Chowdhury, Adam, and Teubner [66] contend that stress and fatigue could also result from cybersecurity and IT technical personnel operating under time pressure in activities such as technology implementations, backups, system updates, and technology migrations, and non-security professionals working under time pressure due to a high workload or a user's perception of the expectations of his supervisor while responding to the supervisor's requests [66].

Hardening systems by implementing new rules and regulations require additional time for policy implementation and training while reducing the time required for performing critical activities, thus increasing stress levels and inadvertently resulting in human vulnerabilities that attackers can exploit [67]. Stress, Burnout, and Security Fatigue can be mitigated with operational countermeasures such as training and awareness programs, security policies and procedures, data backups, simulation of security incidents, and human countermeasures such as improved security culture, behavioral reinforcement, work-life balance, and improved job design [66]. Optimizing regulations to increase system resilience and performance can also allow users more time for their work and thus lead to stress reduction [67].

4.5. Information Security in Nigerian Banks

According to Olalere, Waziri, Ismaila, Adebayo, and Ololade [68] and Ogunwale [69], technological advances have led to the ubiquity of the internet, which has changed the mode of operations of banks with the introduction of internet banking, though with its associated issues in information security. The study conducted by Olalere, Waziri, Ismaila, Adebayo, and Ololade [68] on information security awareness among online banking customers in Nigeria indicated that most customers were unaware of the risk associated with phishing attacks and password cracking, although there was some awareness of the dangers of sharing passwords with others. This finding was collaborated on by Garba and Bade [66], who found that the lack of awareness on the part of employees was a key factor in the cybersecurity issues in Nigeria.

In another study on mitigating cybersecurity issues in Nigeria, Adenusi, Adekunle, Ekuewa, and Ayediran [71] contend that cybercrime has increased exponentially in recent times, partly due to increased digitalization in the banking sector, and therefore advocate that both technology solutions, as well as training and awareness programs, should be adopted. Similarly, Omodunbi, Odiase, Olaniyan, and Esan [72], in their study on cybercrimes in Nigeria, reported that cybercrimes are on the increase, with a majority of perpetrators using phishing as their attack vector leading to the loss of money and disclosure of personal information. They, therefore, suggested that Nigeria should improve the well-being of its citizens and the reorientation and education of its population, especially the youth. Another reason adduced for the increasing wave of cybercrimes in Nigeria is the lack of prosecution of cybercrime offenders by the management of banks [73].

The contention that cybersecurity issues are on the rise in Nigerian banks is also supported by Wang, Nnaji, and Jung [74], who concluded that cybersecurity breaches are on the rise, with the attacks being more sophisticated and requiring banks to improve their cybersecurity practices. This rise in cybersecurity issues may be due to many African countries considering cybersecurity a luxury, a situation that is leading to a severe shortage of cybersecurity professionals and an upsurge in cybersecurity threats that require increased investments in cybersecurity and cybersecurity-related training and awareness [75].

In their study of employee behavioral factors that affect information security standard compliance in Nigerian banks, Williams, Maharaj, and Ojo [60] reported that certainty of detection, penalties, subjective norm, self-efficacy, security awareness of information security threats, and perceived effectiveness of security policies had positive effects on information security policy compliance.

To curb cybercrimes in Nigeria, [69] recommends using strong passwords that are changed periodically and deploying anti-malware solutions. Furthermore, information security policies should be written in simple language, and employees should be trained while managers should ensure the compliance of their subordinates [60].

4.6. Summary of Findings

Table 2 summarizes this study's findings and the suggested mitigants that can be applied.

Table 2. Summary of Findings

Category	Human Factor	Mitigant	Authors
Social Engineering (Phishing, Dumpster Diving, Scareware, Water Hole, Reverse social engineering, Deepfake)	Deception & Manipulation (due to lack of knowledge, lack of resources, lack of awareness, organizational norms, and complacency); Prevalence effect	Training (face-to-face, self-directed, teachable moments); Phishing simulations; Avoiding work overload; Changing user interfaces; Addressing user attitudes and behaviors; Introducing frameworks and models that improve user security; Instituting proper cyber security and communication policies; Implementing anti-phishing protection guidelines; Emphasizing the perceived threats from cyber-attacks.	Fabio, Magalini, Casaroli, Mari, Dixon & Coventry (2022); Hadlington (2017); Huang & Zhu (2022); Desolda, Ferro, Marrella, Catarci, & Costabile (2021); Nifakos, et al. (2021); Alhashmi, Darem & Abawajy (2021); Siddiqi, Pak & Siddiqi (2022); Connolly & Wall (2019); Alsharif, Mishra & AlShehri (2022); Weaver, Braly & Lane (2021); Proctor & Chen (2015); Sawyer & Hancock (2018); Klimburg-Witjes & Wentland (2021); Chaudhary, Berki, Li & Valtanen (2015); Vrhovec, Bernik & Markelj (2023)
Risky Password Practices	Using default or weak passwords; Recycling passwords	Adopting complex passwords with expiration dates or longer passwords and passphrases; Applying password history; Changing passwords routinely	Hadlington (2017); Al-Slais & El-Medany (2022); Grobler, Chamikara, Abbott, Jeong, Nepal & Paris (2021); Alsharif, Mishra & AlShehri (2022); Neigel, Claypoole, Waldfogle, Acharya & Hancock (2020); Kennison & Chan-Tin (2020)

Category	Human Factor	Mitigant	Authors
Poor information security culture	Negative behavior arising from inducement, manipulation, or coercion.	Training and Awareness	Caire (2017)
Poor information security culture	Lack of adherence to cybersecurity policies due to perception of social approval; Perception of how supervisors treat awareness campaigns; Perception of the efficacy of the awareness campaign; Perception of the overall performance of authorities in dealing with errant behavior	Improved messaging tailored to the target population	Vrhovec, Bernik & Markelj (2023)
Poor information security culture	Lack of compliance with security policies and procedures	Implementing an appropriate combination of rewards and punishments; Education and Awareness; Designing work tools, security policies, and procedures not to impede user experience or the realization of organizational goals.	Parsons, Young, Butavicius, McCormac, Pattinson & Jerram (2015); Abdalla, Arshad, Jarrah & Abu-Khadrah (2021); Pollini et al. (2022); Kanwal, Shi, Kontovas, Yang & Chang (2022); Caire (2017)
Poor information security culture	Prevalence effect	Expanded and continued investment in understanding the human factor in cybersecurity.	Sawyer & Hancock (2018)
Poor information security culture	Stress, burnout, and security fatigue; Personal issues; Serious mental health disorders; Situational awareness; Policies and role awareness	Engage human factors practitioners to assist in mitigating or eradicating human factors; Implement anti-fatiguing programs.	Nobles (2022); Georgiadou, Mouzakitis & Askounis (2022)
Poor information security culture	Unintentional insider threat due to lack of attention to details; Poor planning and ignorance; Not logging out of computers; Task factors; Accidents; Poor decision making.	Education, awareness, and communication	Hadlington (2021); Triplett (2022); Khan, Houghton & Sharples (2022)
Poor information security culture	Insufficient knowledge and skills	Education and Awareness	Yanakiev & Polimirova (2020); Pollini, et al. (2022); Alsulami, et al. (2021); Szczepaniuk & Szczepaniuk (2022)
Poor information security culture	Mistakes, negligence, greed, or recklessness	Implementing an appropriate combination of rewards and punishments, Education and awareness.	Elifoglu, Abel, & Tasseven (2018)
Poor information security culture	Risky cybersecurity behaviors	Training, cybersecurity awareness; Motivation	Hadlington (2017); Hakami & Alshaikh (2022); Qashqari, Munshi, Alturkstani, Ghwati &

Category	Human Factor	Mitigant	Authors
			Alhebshi (2020)
Stress, burnout, and security fatigue	Stress, burnout, and security fatigue	Engaging human factor experts	Nobles (2022); Lahcen, Caulkins, Mohapatra & Kumar (2020)
Stress, burnout, and security fatigue	Stress exacerbated by unresponsive IT support, Users, and technical personnel working under pressure.	Prompt, responsive, and effective IT support; Training and awareness programs; Implementing security policies and procedures; Ensuring work-life balance and improved job design	Chowdhury, Adam & Skinner (2019); Blythe & Coventry (2018); Chowdhury, Adam & Teubner (2022)
Stress, burnout, and security fatigue	Stress due to hardening systems by introducing additional rules and regulations	Optimizing regulations to increase system resilience and performance leads to stress reduction.	Gisladottir, Ganin, Keisler, Kepner & Linkov (2017)
Information security in Nigerian banks	Lack of awareness	Improve the well-being of Nigerian citizens; Improve cybersecurity practices, training, and awareness.	Olalere, Waziri, Ismaila, Adebayo & Ololade (2014); Garba & Bade (2021); Adenusi, Adekunle, Ekuewa & Ayediran (2020); Omodunbi, Odiase, Olaniyan & (2016); Wang, Nnaji & Jung (2020); Kshetri (2019);

5. Discussion

The internet's widespread presence has led to the globalization of our world, connecting people and businesses across national borders. This increased interconnectedness allows for faster global communication but also opens the door for the rapid spread of cyberattacks. The WannaCry ransomware attack in May 2017, which affected at least 150 countries, including Nigeria, is a prime example of the potential reach and impact of cyber threats. The attack was successful because organizations used outdated and unpatched Microsoft Windows systems, highlighting the human factor in cybersecurity. In fact, incidents caused by careless or negligent insiders accounted for 56% of all cybersecurity incidents in 2022, with the Middle East and Africa experiencing the majority of these events [13]. This high number of incidents is likely due to a lack of cybersecurity resources and awareness in these regions, as studies, for instance, have shown that many bank customers in Nigeria are not aware of the risks associated with phishing attacks and password cracking [68].

Research by Garba and Bade [70] further supports the significance of the human factor in cybersecurity, stating that employee awareness is crucial to addressing cybersecurity issues in Nigeria. Adenusi, Adekunle, Ekuewa, and Ayediran [71] also advocate for implementing both technology solutions and training and awareness programs to mitigate cybersecurity risks in the country.

Phishing remains the preferred attack vector used by cybercriminals in Nigeria [72], reflecting the global trend where phishing is considered the most common social engineering attack vector. To address

this issue, researchers have suggested improving the well-being of citizens and providing reorientation and education, especially for young people [23, 26, 27, 28, 29].

Garba and Bade [70] and Williams, Maharaj, and Ojo [60] reiterate the importance of employee awareness in combating cybersecurity issues in Nigeria, while Adenusi, Adekunle, Ekuewa, and Ayediran [71] stress the need for both technology solutions and training and awareness programs. In a study on employee behavior and information security compliance in Nigerian banks, Williams, Maharaj, and Ojo [60] found that factors such as certainty of detection, subjective norm, self-efficacy, and security awareness positively impacted compliance with information security policies. These findings align with global research on the human factors in cybersecurity, suggesting that Nigerian banks should adopt similar mitigating measures. However, the most effective approach to overcoming the human factor in cybersecurity appears to be implementing training and awareness programs within organizations, which can be conducted cost-effectively through online collaboration tools like Zoom, Microsoft Teams, and Google Meet.

On the other hand, Ponemon Institute research shows that the cost of remediating cyberattacks varies significantly based on the type of incident, with the annualized cost of negligence being the highest at $6.6 million [13]. As a result, while all mitigating measures should be considered, prioritizing training and cybersecurity awareness programs can provide a strong foundation for tackling cyber threats, especially for organizations with limited cybersecurity budgets, such as Nigerian banks.

The human factor in cybersecurity remains a significant concern in the ever-evolving digital landscape. The increasing sophistication and reach of cyber threats, coupled with a lack of awareness and preparedness among employees and organizations, exacerbate the risks associated with cybersecurity. In regions like Nigeria and other parts of the Middle East and Africa, this problem is further magnified due to insufficient resources and a general lack of cybersecurity awareness.

Addressing the human factor in cybersecurity requires a multifaceted approach, including ongoing training and awareness programs, implementing advanced technological solutions, and promoting a culture of shared responsibility within organizations. Focusing on the human aspect not only helps organizations identify and rectify potential vulnerabilities but also empowers employees to take an active role in maintaining a secure environment. Moreover, governments and institutions should invest in education and public awareness campaigns to help individuals understand the risks associated with cyber threats and the importance of adopting secure practices online. Collaborative efforts between governments, private organizations, and international entities can also help build a more robust cybersecurity infrastructure that would benefit everyone involved.

Recognizing the human factor's role in cybersecurity and implementing strategies that address this aspect comprehensively is essential. By focusing on education, training, and raising awareness, governments and organizations such as banks can create a more resilient digital ecosystem that mitigates the impact of cyber threats and fosters a safer online environment for all.

6. Conclusion

An understanding of the human behaviors and factors that contribute to the success or failure of cybersecurity is pertinent and vital and represents a very challenging issue for organizations, as humans are responsible for a majority of cybersecurity incidents [10] since humans must interact with technology to achieve the desired results. These human factors, which are the main motivating factors for insider attacks, are usually due to personality traits, human emotions, financial needs, external loyalties, knowledge and skills, interconnectedness, and organizational culture [20].

Following the review of the extant literature on human factors in cybersecurity, these factors are categorized into social engineering; poor information security culture; risky password practices; stress, burnout, and security fatigue. Although very little research has been conducted on the issue of human factors in cybersecurity in Nigerian banks, findings from the review of literature on human factors in

cybersecurity and studies on cybersecurity and cybercrime in Nigeria indicated that the factors categorized under the four sections are also applicable to Nigerian banks.

Resolving cybersecurity incidents arising from human factors can lead to significant annual expenses of between $4.1 and $6.6 million, depending on the nature of the incident. Given this considerable cost for remediation, Nigerian banks need to pay attention to the mitigation measures highlighted in this study, starting with training and cybersecurity awareness using approaches such as face-to-face, self-directed, teachable moments and phishing simulations while ensuring that these measures are tailored to the target population as training and awareness can provide a solid basis for tackling cyber-attacks, especially for organizations without a large cybersecurity budget. Instituting and implementing proper cyber security and communication policies and anti-phishing protection guidelines would also assist these banks in improving their cybersecurity practices. These measures can then be followed up by addressing user attitudes and behaviors, introducing frameworks and models that improve user security, avoiding work overload, and ensuring that work tools, security policies and procedures, and user interfaces are designed not to impede user experience or the realization of organizational goals. Implementing an appropriate combination of rewards and punishments should also be considered.

References

[1] M. A. Adesola, O. A. Moradeyo and K. O. Oyeniyi, "Impact Of Information And Communication Technology On Nigerian Banks Operations A Study Of United Bank For Africa (UBA) Plc," *International Journal of Business and Management Invention,* vol. 2, no. 9, pp. 7-12, 2013.

[2] N. P. Nwakoby, C. P. Sidi and O. S. Abomeh, "Impact of Information and Communication Technology on the Performance of Deposit Money Banks," *International Journal of Management and Sustainability,* vol. 7, no. 4, pp. 225-239, 2018.

[3] S. Mohurle and M. Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017," *International Journal of Advanced Research in Computer Science,* vol. 8, no. 5, pp. 1938-1940, 2017.

[4] M. Akbanov, V. G. Vassilakis and M. D. Logothetis, "Ransomware Detection and Mitigation using Software-Defined Networking: The Case of WannaCry," *Computers & Electrical Engineering,* vol. 76, pp. 111-121, 2019.

[5] J. M. Blythe and L. Coventry, "Costly but effective: Comparing the factors that influence employee anti-malware behaviours," *Computers in Human Behavior,* vol. 87, pp. 87-97, 2018.

[6] C. Nobles, "Botching Human Factors in Cybersecurity in Business Organizations," *Holistica,* vol. 9, no. 3, pp. 71-88, 2018.

[7] E. Kadena and M. Gupi, "Human Factors in Cybersecurity: Risks and Impacts," *Security science journal,* vol. 2, no. 2, pp. 51-64, 2021.

[8] V. Linkov, P. Zámecˇník, D. Havlícˇková and C.-W. Pai, "Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research," *Frontiers in Psychology,* vol. 10, pp. 1-7, 2019.

[9] I. Al-Shanfari, W. Yassin, N. Tabook, R. Ismail and A. Ismail, "Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees," *International Journal of Advanced Computer Science and Applications,* vol. 13, no. 8, pp. 479-490, 2022.

[10] M. Hakami and M. Alshaikh, "Identifying Strategies to Address Human Cybersecurity Behavior: A Review Study," *International Journal of Computer Science and Network Security,* vol. 22, no. 4, pp. 299-309, 2022.

[11] ENISA, "Cyber security culture in organisations," European Union Agency for Network and Information Systems, 2018.

[12] L. Y. Connolly, D. S. Wall, M. Lang and B. Oddson, "An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability," *Journal of Cybersecurity,* vol. 6, no. 1, pp. 1-18, 2020.

[13] Ponemon, "2022 Cost of Insider Threats Global Report," 2022.

[14] NIBSS, "Fraud in the Nigerian Financial Services," [Online]. Available: https://nibss-plc.com.ng/nibss-insight-fraud-in-the-nigeria-financial-services/

[15] ISO, "ISO/IEC 27032:2012(en) Information technology — Security techniques — Guidelines for cybersecurity," 2012. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en. [Accessed 10 March 2023].

[16] NIST, "Computer Security Resource Center," [Online]. Available: https://csrc.nist.gov/glossary/term/cybersecurity. [Accessed 11 April 2023].

[17] T. Emmersen, J. M. Hatfield, J. Kosseff and S. R. Orr IV, "The USNA's Interdisciplinary Approach to Cybersecurity Education," *Computer,* vol. 52, no. 3, pp. 48-57, 2019.

[18] C. Qian, P. Romanowich, J. Castillo, K. C. Roy, G. Chavez and S. Xu, "ExHPD: Exploiting Human, Physical, and Driving Behaviors to Detect Vehicle Cyber Attacks," *IEEE Internet of Things Journal,* vol. 8, no. 18, pp. 14355-14371, 2021.

[19] R. A. M. Lahcen, B. Caulkins, R. Mohapatra and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity,* vol. 3, no. 1, pp. 1-18, 2020.

[20] S. Prabhu and N. Thompson, "A primer on insider threats in cybersecurity," *Information Security Journal: A Global Perspective,* vol. 31, no. 5, pp. 602-611, 2022.

[21] M. Antunes, C. Silva and F. Marques, "An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context," *Applied Sciences,* vol. 11, no. 23, p. 11269, 2021.

[22] L. Y. Connolly and D. S. Wall, "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures," *Computers & Security,* vol. 87, 2019.

[23] M. Alsharif, S. Mishra and M. AlShehri, "Impact of Human Vulnerabilities on Cybersecurity," *Computer Systems Science & Engineering,* vol. 40, no. 3, pp. 1153-1166, 2022.

[24] L. Huang and Q. Zhu, "RADAMS: Resilient and Adaptive Alert and Attention Management Strategy against Informational Denial-of-Service (IDoS) Attacks," *Computers & Security,* 2022.

[25] M. A. Siddiqi, W. Pak and M. A. Siddiqi, "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures," *Applied sciences,* vol. 12, no. 12, p. 6042, 2022.

[26] R. Fabio, S. Magalini, A. Casaroli, P. Mari, M. Dixon and L. Coventry, "Phishing simulation exercise in a large hospital: A case study," *Digital Health,* vol. 8, pp. 1-13, 2022.

[27] A. A. Alhashmi, A. Darem and J. H. Abawajy, "Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats," *International Journal of Advanced Computer Science and Applications,* vol. 12, no. 10, pp. 29-35, 2021.

[28] S. Nifakos, K. Chandramouli, K. C. Nikolaou, P. Papachristou, S. Koch, E. Panaousis and S. Bonacina, "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review," *sensors,* vol. 21, no. 15, p. 5119, 2021.

[29] B. W. Weaver, A. M. Braly and D. M. Lane, "Training Users to Identify Phishing Emails," *Journal of Educational Computing Research,* vol. 59, no. 6, pp. 1169-1183, 2021.

[30] R. W. Proctor and J. Chen, "The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace," *Human factors,* vol. 57, no. 5, pp. 721-727, 2015.

[31] B. D. Sawyer and P. A. Hancock, "Hacking the Human: The Prevalence Paradox in Cybersecurity," *Human factors,* vol. 60, no. 5, pp. 597-609, 2018.

[32] G. Desolda, L. S. Ferro, A. Marrella, T. Catarci and M. F. Costabile, "Human Factors in Phishing Attacks: A Systematic Literature Review," *ACM Computing Surveys (CSUR),* vol. 54, no. 8, pp. 1-35, 2021.

[33] N. Klimburg-Witjes and A. Wentland, "Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses," *Science, Technology, & Human Values,* vol. 46, no. 6, pp. 1316-1339, 2021.

[34] S. Vrhovec, I. Bernik and B. Markelj, "Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign," *Computers & Security,* vol. 125, p. 103038, 2023.

[35] S. Chaudhary, E. Berki, L. Li and J. Valtanen, "Time Up for Phishing with Effective Anti-Phishing Research Strategies," *International Journal of Human Capital and Information Technology Professionals,* vol. 6, no. 2, pp. 49-64, 2015.

[36] M. Grobler, M. A. P. Chamikara, J. Abbott, J. J. Jeong, S. Nepal and C. Paris, "The importance of social identity on password formulations," *Personal and Ubiquitous Computing,* vol. 25, no. 5, p. 813–827, 2021.

[37] Y. Al-Slais and W. El-Medany, "User-Centric Adaptive Password Policies to Combat Password Fatigue," *The International Arab Journal of Information Technology,* vol. 19, no. 1, pp. 55-61, 2022.

[38] L. Hadlington, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon,* vol. 3, no. 7, p. e00346, 2017.

[39] S. M. Kennison and E. Chan-Tin, "Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors," *Frontiers in Psychology,* vol. 11, p. 546546, 2020.

[40] A. R. Neigel, V. L. Claypoole, G. E. Waldfogle, S. Acharya and G. M. Hancock, "Holistic cyber hygiene education: Accounting for the human factors," *Computers & Security,* vol. 92, p. 101731, 2020.

[41] A. Georgiadou, S. Mouzakitis, K. Bounas and D. Askounis, "A Cyber-Security Culture Framework for Assessing Organization Readiness," *Journal of Computer Information Systems,* vol. 62, no. 3, pp. 452-462, 2022.

[42] K. M. Parsons, E. Young, M. A. Butavicius, A. McCormac, M. R. Pattinson and C. Jerram, "The Influence of Organizational Information Security Culture on Information Security Decision Making," *Journal of Cognitive Engineering and Decision Making,* vol. 9, no. 2, pp. 117-129, 2015.

[43] A. Pollini, T. C. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi and D. Guerri, "Leveraging human factors in cybersecurity: an integrated methodological approach," *Cognition, Technology & Work,* vol. 24, no. 2, p. 371–390, 2022.

[44] M. Abdalla, Y. b. Arshad, M. Jarrah and A. Abu-Khadrah, "Factors Influencing the Adoption of Cyber Security Standards Among Public Listed Companies in Malaysia," *International Journal of Advanced Computer Science and Applications,* vol. 12, no. 11, pp. 804-810, 2021.

[45] J. Caire, "Human Factors in Cybersecurity for Transportation Systems," *WIT Transactions on The Built Environment,* vol. 176, pp. 405-414, 2017.

[46] M. Fagan and M. M. H. Khan, "To Follow or Not to Follow: A Study of User Motivations around Cybersecurity Advice," *IEEE Internet Computing,* vol. 22, no. 5, pp. 25-34, 2018.

[47] S. J. Philip, T. J. Luu and C. Traci, "There's No place like home: Understanding users' intentions

toward securing internet-of-things (IoT) smart home networks," *Computers in Human Behavior,* vol. 139, p. 107551, 2023.

[48] N. Wulandari, M. S. Adnan and C. B. Wicaksono, "Are You a Soft Target for Cyber Attack? Drivers of Susceptibility to Social Engineering-Based Cyber Attack (SECA): A Case Study of Mobile Messaging Application," *Human Behavior and Emerging Technologies,* 2022.

[49] L. Hadlington, "The "human factor" in cybersecurity: Exploring the accidental insider," in *Research anthology on artificial intelligence applications in security*, IGI Global, 2021, pp. 1960-1977.

[50] W. J. Triplett, "Addressing Human Factors in Cybersecurity Leadership," *Journal of Cybersecurity and Privacy,* vol. 2, no. 3, pp. 573-586, 2022.

[51] Y. Yanakiev and D. Polimirova, "Exploring the Role of the Human Factor in Cybersecurity: Results from an Expert Survey in Bulgaria," *Information and Security,* vol. 44, pp. 39-50, 2020.

[52] M. H. Alsulami, F. D. Alharbi, H. M. Almutairi, B. S. Almutairi, M. M. Alotaibi, M. E. Alanzi, K. G. Alotaibi and S. S. Alharthi, "Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia," *Information,* vol. 12, no. 5, p. 208, 2021.

[53] I. H. Elifoglu, I. Abel and Ö. Tasseven, "Minimizing Insider Threat Risk with Behavioral Monitoring," *Review of business,* vol. 38, no. 2, pp. 61-73, 2018.

[54] G. Mazzarolo and A. D. Jurcut, "Insider threats in Cyber Security: The enemy within the gates," *arXiv preprint arXiv:1911.09575,* 2019.

[55] N. Khan, R. J. Houghton and S. Sharples, "Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks," *Cognition, Technology & Work,* vol. 24, pp. 393-421, 2022.

[56] K. Kanwal, W. Shi, C. Kontovas, Z. Yang and C.-H. Chang, "Maritime cybersecurity: are onboard systems ready?," *Maritime Policy and Management,* pp. 1-19, 2022.

[57] E. K. Szczepaniuk and H. Szczepaniuk, "Analysis of cybersecurity competencies: Recommendations for telecommunications policy," *Telecommunications Policy,* vol. 46, no. 3, p. 102282, 2022.

[58] A. A. Qashqari, A. M. Munshi, H. A. Alturkstani, H. T. Ghwati and D. H. Alhebshi, "The Human Factors and Cybersecurity Policy," *International Journal of Computer Science and Network Security,* vol. 20, no. 4, 2020.

[59] A. Georgiadou, S. Mouzakitis and D. Askounis, "Detecting Insider Threat via a Cyber-Security Culture Framework," *Journal of Computer Information Systems,* vol. 62, no. 4, pp. 706-716, 2022.

[60] A. S. Williams, M. S. Maharaj and A. I. Ojo, "Employee Behavioural Factors and Information Security Standard Compliance in Nigeria Banks," *International Journal of Computing and Digital Systems,* vol. 8, no. 04, pp. 387-396, 2019.

[61] X. Chen, D. Wu, L. Chen and J. K. L. Teng, "Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables," *Information & Management,* vol. 55, no. 8, pp. 1049-1060, 2018.

[62] T. Mohammad, N. A. M. Hussin and M. H. Husin, "Online safety awareness and human factors: An application of the theory of human ecology," *Technology in Society,* vol. 68, p. 101823, 2022.

[63] R. S. Dalal, D. J. Howard, R. J. Bennett, C. Posey, S. J. Zaccaro and B. J. Brummel, "Organizational science and cybersecurity: abundant opportunities for research at the interface," *Journal of Business and Psychology,* vol. 37, no. 1, p. 1–29, 2022.

[64] C. Nobles, "Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem," *Holistica,* vol. 13, no. 1, pp. 49-72, 2022.

[65] N. H. Chowdhury, M. T. P. Adam and G. Skinner, "The impact of time pressure on cybersecurity behaviour: a systematic literature review," *Behaviour & Information Technology,* vol. 38, no. 12, pp.

1290-1308, 2019.

[66] N. H. Chowdhury, M. T. Adam and T. Teubner, "Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures," *Computers & Security*, vol. 97, p. 101931, 2022.

[67] V. Gisladottir, A. A. Ganin, J. M. Keisler, J. Kepner and I. Linkov, "Resilience of Cyber Systems with Over- and Underregulation," *Risk Analysis*, vol. 37, no. 9, pp. 1644-1651, 2017.

[68] M. Olalere, V. O. Waziri, I. Ismaila, O. S. Adebayo and O. Ololade, "Assessment of Information Security Awareness among Online Banking Costumers in Nigeria," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 6, pp. 13-24, 2014.

[69] H. Ogunwale, "The Impact of Cybercrime on Nigeria's Commercial Banking System," *International Journal of Management and Business Studies*, vol. 2, no. 3, pp. 75-78, 2020.

[70] A. A. Garba and A. M. Bade, "The Current State of Cybersecurity Readiness in Nigeria organizations," *International Journal of Multidisciplinary and Current Educational Research (IJMCER)*, vol. 3, no. 1, pp. 154-162, 2021.

[71] D. A. Adenusi, A. U. Adekunle, J. B. Ekuewa and O. R. Ayediran, "Challenges and Ways out of Cyber Security Issues in Nigeria," *Villanova Journal of Science, Technology and Management*, vol. 2, no. 1, pp. 2672-4987, 2020.

[72] B. A. Omodunbi, P. O. Odiase, O. M. Olaniyan and A. O. Esan, "Cybercrimes in Nigeria: Analysis, Detection and Prevention," *FUOYE Journal of Engineering and Technology*, vol. 1, no. 1, pp. 37-42, 2016.

[73] B. M. Ololade, M. K. Salawu and A. D. Adekanmi, "E-Fraud in Nigerian Banks: Why and How?," *Journal of Financial Risk Management*, vol. 9, no. 3, pp. 211-228, 2020.

[74] V. Wang, H. Nnaji and J. Jung, "Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability," *International Journal of Law, Crime and Justice*, vol. 62, p. 100415, 2020.

[75] N. Kshetri, "Cybercrime and Cybersecurity in Africa," *Journal of Global Information Technology Management*, vol. 22, no. 2, pp. 77-81, 2019.