:: IJEBD ::
(International Journal of Entrepreneurship and Business Development)
Volume 06 Number 05 September 2023

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

Effect of Cyber Security on Business Sustainability of Listed Microfinance Banks in Nigeria

Cosmas Anayochukwu Nwankwo and Macdonald Isaac Kanyangale
University of KwaZulu-Natal, South Africa
Corresponding Author*: j.cosmaris@gmail.com, kanyangalem@ukzn.ac.za

ABSTRACT

Purpose: In Nigeria, microfinance banks (MFB) face the burden of investing in cyber security to protect their databases, prevent monetary losses, maintain customer trust, and remain afloat in a competitive business environment. However, there are incessant cyber risks and attacks by criminals who gain undue access to the cyber-space of MFB and cause financial and non-financial loss.

Design/methodology/approach: The objective of this quantitative study was to examine the effect of cyber security on the business sustainability of three listed, and most valued MFBs in Nigeria. The population of the study was 315 senior, medium and junior employees of three MFBs in Nigeria. As the target population was manageable, the research adopted a census. Data were collected using a semi-structured questionnaire, and the formulated hypothesis was analysed using multiple regression.

Findings: The study found that cyber security has a significant and positive impact on the sustainability of MFB in Nigeria. Data availability account for the largest contribution to the sustainability of MFBs, followed by data confidentiality and data integrity. Employees in a MFB uphold that data availability, confidentiality, and integrity are pivotal elements of cyber security that influence the sustainability of their organisations in Nigeria. Given these results from the viewpoint of employees, MFBs are implored to regularly review and strengthen their risk management strategy and adopt a more integrative approach of human-centric cybersecurity, which brings technology and human elements together to address current and future cyber risks and build and sustain consumer trust in digital financial transactions. The implication of the study and areas for future research are highlighted.

Paper type: Research paper

Keyword: *Cyber Security, Business Sustainability, Listed Microfinance Banks, Nigeria*
Received : June 8th
Revised : August 18th
Published : September 30th

I. INTRODUCTION

In the 21st century, more Micro finance banks (MFBs) are offering services and conducting operations in a highly sophisticated environment where business sustainability faces various security hazards from internal and external cyber-attacks (Perwej, Abbas, Dixit, Akhtar & Jaiswal, 2021). The sophistication and systemic risks of cyber-attacks necessitate the persistent need for Micro finance Banks (MFBs) to safeguard data and other organisational resources from hacker operations to ensure business sustainability. Xu, Fu and Liu (2019:1) assert that.

"MFB distinguishes itself from traditional financial institutions, such as the commercial bank, by operating small loans to "unbankable poor people and small businesses", is not only considered an effective way for the poor to manage their finances and take advantage of economic opportunities while managing risks, but also an important way to promote economic development, employment and growth, through the financial support of small businesses".

Since Bangladesh introduced the microfinance banking system in the middle of the 1970s, several other nations, especially third-world countries, have copied similar financial strategies or models. The potential for poverty reduction is the basis for the micro finance model's apparent popularity in emerging nations. In Nigeria, the acronyms of MFI and MFB are used to mean the type of organisation and provider of micro finance services.

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

Over the years, the business survival of MFBs is undermined by the growth and variety of crimes conducted through digital technologies (Seemma, Nandhini & Sowmiya, 2018). Morgan (2020) warned that cybercrime is expected to cause about six trillion dollars in worldwide damage by 2025 if not well managed in the global economy. The buoyant digital economy thrives on stable, safe, resilient and dynamic cyberspace for financial service providers and businesses.

Digitalising services to achieve higher efficiency, increased productivity, lower operating costs, improved customer experience, and enhanced competitive advantage are topics relevant to cybersecurity researchers and MFBs. First, cyber threats and attacks against MFBs can negatively impact the sustainability model of MFB (Miracle, Armah, Mohammed & Sackey-Sam, 2021). Payments, withdrawals, deposits, and fund transfers between banks are among the banking operations that are financially disrupted by security breaches in MFIs.Non-financial consequences of cyber-attack include losing clients' trust in the banks' ability to protect their money and private information, legal actions, and compensation claims from the affected clients or third parties.

Second, MFB faces the burden of enhancing cyber security, which is evident in additional cyber overhead costs to build cyber-resilient technology infrastructure adequately. Generally, it is anticipated that by 2025, global cyber security spending will hit $200bn, which would have been re-directed and reinvested for better economic development but is budgeted for fighting cybercrimes and internet-related risks (Morgan, 2020). For MFBs, there is a chance that excessive investment in cyber technology will wipe out the marginal profits and harm their capacity to sustain their finances. Due to the rising digitalisation of banking operations and the systemic danger of technology, it might be argued that MFBs must significantly boost their spending on cyber technology. A breach in the network of MFB might bring down the entire integrated banking system. In this way, systemic cyber security hazards escalate operational risks, adversely affecting the financial results of financial institutions like banks. Experts in cyber security face a dilemma in determining the best investment to make in MFB's cyber security infrastructure to slow the spread of cybercrime.

Nigeria was ranked 47th on the global cyber security index (GCI) in 2020. Cybercriminals in Nigeria are not just sharpening their cyber skills but also busy scaling up by training new and younger people in various types of internet frauds (e.g. love frauds, online trading frauds, and identity theft) to inflict colossal losses and financial burdens on vulnerable MFIs (Aragba-Akpore,2022). "Yahoo yahoo" is a term for internet fraud that has become common in Nigeria (Aragba-Akpore, 2022). As a result of cybercrimes, Nigerians across the globe have a negative image as they are always perceived as fraudsters.

There is a relative ease with which criminals in Nigeria can learn the necessary cyber skills. On the other hand, it is startling that businesses in Africa repeatedly lament the unavailability of individuals with the essential skills to implement appropriate cybersecurity controls in organisations (Miracle, Armah, Mohammed & Sackey-Sam, 2021). Web and mobile security, security operations, and incident management are the three areas where cybersecurity practitioners have the most knowledge gaps (Catal, Ozcan, Donmez & Kasif, 2022). Detection of intrusion and secure software development is the most challenging skill for organisations (Catal, Ozcan, Donmez & Kasif,2022).

Lastly, both MFB and small and medium enterprises (SMEs) are attractive targets for cybercriminals. SMEs are targeted because they neither have the reserves, resources, nor sufficient skill levels of employees to build and maintain robust security measures against cyber threats (Duncan & Westerlund, 2022). Cybercriminals consider MFBs attractive because of financial gains and a systemic risk that allows them to access customer data, corporate espionage, or massive customer attacks through networks (Duncan & Westerlund, 2022).

Integration of technical and non-technical measures (e.g. policy development, regulatory compliance, external collaboration, organisational reform, and capacity building) as part of cyber security management practices is vital as no technology system is free from cybercrimes. As technology evolves, cyber investment is a strategic necessity for MFBs to undermine any innovative cybercrime practices (Miracle, Armah, Mohammed & Sackey-Sam, 2021).

Scholars such as Uddin, Ali, and Hassan (2020) have investigated (i) how cyber security risks increase banks' operational costs, (ii) how security lapses affect institutions' performance, (iii) how broadly applying cyber technology increases operational risk, and (iv) the current practises of cyber security disclosure and governance. However, Garcia-Perez et al. (2020:2) underscore that “microfinance has been scarcely investigated from the point of view of sustainability or its impact on sustainable development, where the contexts of the regions should be considered”.

While extant research in Nigeria has widely delved into the relationship between cyber security, Microfinance Banks (MFBs) growth, and sustainability in the past few years, there is a limited link to SMEs. Yakubu (2017) investigated the methods of cybercrime, identified reasons for cybercrime, and the possible ways it could be reduced if not eradicated. Omodunbi, Odiase, Olaniyan, and Essan (2016) evaluated the level of students' involvement in cybercrimes. Therefore, there is a compelling need to understand the cyber security and sustainability of MFBs as a critical aspect of the financial sector and the Nigerian cyber environment.

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

The objective of this study is to examine the effect of cyber security on the business sustainability of MFBs in Nigeria. In line with the objective of the study, the hypothesis for this study is stated below:

H01: Cybersecurity has no significant effect on the business sustainability of MFBs in Nigeria.

The article begins by unpacking the cyber security concept and confidentiality, integrity and availability (CIA) triad cybersecurity model before focusing on business sustainability in MFBs. The article discusses the research methodology, results and discussion. Lastly, the chapter presents managerial implications and areas of future research. The current study is valuable for micro finance practitioners as it enhances their understanding of how confidentiality, integrity and availability of data are foundational in the provision of digital financial service in ways that positively affect business sustainability in MFBs. The study is equally valuable as it pronounces the need to shift from the orientation of cyber security as tech and exclusive to a more integrative, multi-stakeholder orientation and human centric cyber security.

A. Literature Review

In this study, it is critical to gain clarity on cyber security and business sustainability as crucial concepts relevant to MFI.

1. Unpacking the concept of cyber security

The concept of cyber security has been defined in different ways by scholars such as Chang and Coppel (2020) and Perwej et al. (2021:673), but there is no consensus. Illegal and unauthorised access, safeguarding of the digital system, risks in internet-connected systems, cyber-attacks, cybercrimes and cyber terrorism are common aspects in scholarly efforts to define the phenomenon of cyber security. Individuals and businesses employ techniques to guard against illegal access to data centres and other digital systems. In many ways, the internet has shrunk the world, but it has also exposed the business to fresh obstacles in the online environment.

For example, Perwej et al. (2021:673) construe that "cyber security is a set of strategies and processes for defending computers, networks, databases, and applications against assaults, illegal access, modification, or destruction". Lowering the danger of cyber-attacks and protecting businesses and individuals against unauthorised, unwarranted access and illegal use of systems, networks, and technology is the core of effective cyber security. According to Chang and Coppel (2020), cyber security protects electronic systems, networks, computers, servers, mobile devices, and data from harmful attacks. Some scholars, such as Chang and Coppel (2020), surmise cyber security as information technology or electronic information security. However, it is vital to realise how broad cyber security embraces various contexts (e.g. mobile, business computing) and activities. Cyber security includes a variety of aspects such as (1) network security (protecting a computer network from intruders), (2) application security (keeping the software and devices safe from threats), (3) information security (protecting the integrity and privacy of data while it is in storage and transit), (4) operational security (protecting processes and decisions for handling and protecting data assets), and (5) disaster recovery and business continuity response to a cyber-security incident, restoration.

a. Cyber security risks and cost

Uddin, Ali and Hassan (2020:239) assert that "cyber security risk occurs because institutions are often unable to ensure an appropriate set of tools, technologies, training, and best practices to protect networks, devices, programs, and data from unauthorised access" in the virtual environment. Cyber security and cybercrime are two interdependent, opposing sides of the same coin. One cannot discuss cybersecurity without mentioning cybercrime and the risks it poses to businesses. It is important to emphasise that cyber-security can fend against three threats. First, cybercrime involves lone actors and groups who target systems for harm or financial benefit. Second, political information collection frequently goes hand in hand with cyberattacks.

Last but not least, cyberterrorism aims to disrupt electronic networks to spread fear or panic. Cybersecurity is a target for malicious actors in many ways. Therefore, training employees is essential to creating a more durable operational infrastructure.

According to Morgan (2020), the costs of cybercrime include data loss and destruction, financial loss, increased production costs, intellectual property losses, theft of personal, corporate, and financial data, financial fraud, disruption of regular business operations, programmes, and processes, high-cost forensic investigation, high costs for the restoration and deletion of hacked data, and, most importantly, reputational damage to the institutions and society at large. All organisations must lessen cybercriminal activities of external and internal parties that want to acquire unauthorised access to compromise the integrity and confidentiality of information in a virtual environment as Nigeria transitions to a cashless society (Miracle, Armah, Mohammed & Sackey-Sam, 2021).

Anoke and Ndubuisi-okolo (2022) opined that cryptocurrency, and the just-introduced e-Naira, a new type of technology platform for virtual trading currencies and other transactions, confirm the rapid worldwide technological expansion and the need to regulate these activities. Ebelogu, Ojo, Andeh, and Agu (2019) claim that Nigeria has many cybercrimes, including online fraud, software piracy, hacking, online scams, ATM or credit

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

card fraud, virus distribution, phishing, cyber-stalking, and cyber-defamation. E-banking fraud has undergone a parallel digital revolution to that of e-banking. The dilemma of MFB is that while cyber security adversely impacts cyber overhead costs, cybercrimes create direct losses from cyber security breaches (Anoke, Nzewi, Agagbo, & Onu, 2021).

In this study, cyber security is defined as a set of procedures and actions designed to safeguard the safety of individual and corporate data, networks, and information against any dangers, threats, cyber-attack, and cyber-crime that may arise internally or externally in an organisation. This definition is used because it enables the study to properly dissect cybersecurity concerning microfinance banks' sustainability in an emerging economy like Nigeria.

b. Confidentiality, Integrity and Availability (CIA triad model of cybersecurity

The three broad components of data and information are confidentiality, integrity, and availability, otherwise called the CIA triad (Prakash,2022). In the CIA, Prakash (2022) is explicit that three constitute elements together form the information security concept known as the CIA triad. Each element stands for a core goal of information security.

Firstly, confidentiality in cybersecurity is about access control for data users to prevent unauthorised activities (Prakash,2022). In this regard, consideration is paid to both the sensitivity of the material and who should have access to it when information is. The variety of techniques used for confidentiality includes secrecy classified from public to top secret, authorisations and access rights according to the nature of their job, use of passwords, encryption, locks and keys, and safes. On the other hand, various methods, including social engineering and hacking, may be used to violate confidentiality. Confidentiality measures used in an MFI mustn't inhibit data transfer and sharing processes to be responsive to user needs. It is unreasonable to lock everything down, stop all communications, and limit employee access to the least amount of data necessary to perform their tasks and make services available to users.

Secondly, data integrity is the guarantee or certainty that the data has not been corrupted or changed before, during, or after submission (Prakash,2022). Similarly, Popescul and Cuza (2011) define integrity as keeping data and information in the correct and complete form and must not be modified without authorisation, either accidentally or on purpose. Data integrity hinges on the need to avoid any unauthorised change or compromise during the upload or transmission of data or the document's storage in the database or collection.

Lastly, availability means that the data is easily accessible to authorised users (Prakash,2022). Accessibility refers to assuring access to data and information, for authorised users, at any time. The well-functioning of the hardware equipment and the networks, back-ups (e.g. power generation, safety systems) and observance of laws all lead to availability. Availability also relates to the resilience of processes and systems against cyberattacks and safeguards against hardware failure, power outages, and other situations compromising the system's availability when users need it. Figure 1 depicts the components of information security and how they interact and reinforce each other to ensure cybersecurity.

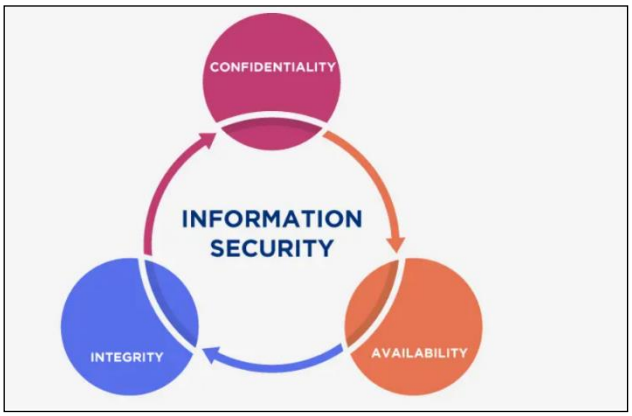

Figure 1: Components of the CIA Model in cybersecurity

Source: Prakash (2022).

Data and information for every organisation typically come from various sources, including operational and information technology and personal and operational data. These data and information must be appropriately

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

managed and always protected. According to Prakash (2022). one of the limitations of the CIA triad is that it is specific and restricted to data. Additionally, the CIA triad does not offer suggestions for building a comprehensive security model for an organisation (Prakash,2022). Furthermore, the CAI triad focuses on data and information security, yet some employees are knowledge workers who require more knowledge than data security. Given the above discussion, this study adopted the CIA triad to operationalise cybersecurity.

2. Dimensions of Business Sustainability

The notion of "business sustainability and sustainable MFB has multi-dimensional elements traceable to the Brundtland Report for the World Commission on Environment and Development (1987:8). Generally, the report echoes that sustainability is about "meeting the needs of the present without compromising the ability of future generations to meet their own needs". At its core, sustainability implies the continued flourishing of human societies in a constantly changing world with competing for social, economic and environmental conditions. The triple bottom line approach (TBL) exhibits that sustainability is complex. It centres around three domains: social, economic and ecological. In this regard, sustainability's environmental aspect includes reducing people's negative environmental impacts and protecting nature and ecosystems (Tsaia & Lu, 2021). Humans must act responsibly and sensitively to use all resources as they have a limit. The economic dimension relates to the link between economic activities, growth, and effects, while the social dimension refers to human, institutional, cultural, and societal aspects. The three spheres of sustainability are interdependent and interconnected and interact in non-linear ways. A shift in one can, in turn, cause a series of knock-on effects in the others.

In a different vein, four dimensions of sustainability proposed by Ashrafi, Acciaro, Walker, Magnan and Adams (2019) are (1) environmental-based sustainability, (2) corporate sustainability, (2) business-related sustainability, and (4) sustainability in education.

Sustainable business requires managers and employees to see themselves as part of a larger organisational, social and ecological system. Business sustainability means businesses should create wealth and improve people's lives. When the microfinance banking program was launched in Nigeria in 2005, the system was put in place to give employment, encourage rural development, alleviate poverty, and supply funding to economically active people who were excluded from the conventional financial markets (Okonkwo & Okeke, 2019).

Notably, some notions of sustainability in strategy have little to do with society as it is only about business. In this case, successfully running a business such as MFI is not sustainable if it entails sacrificing the future for present gains (Anoke, 2019). Both internal and external macro-environmental elements, such as macroeconomics, information technology, and financial sector environments, impact MFB's success (Fashagba, 2018).

Figure 2 below depicts how MFB, the micro-finance institution (MFI), interacts with the social and economic system and constitutes the financial sector.

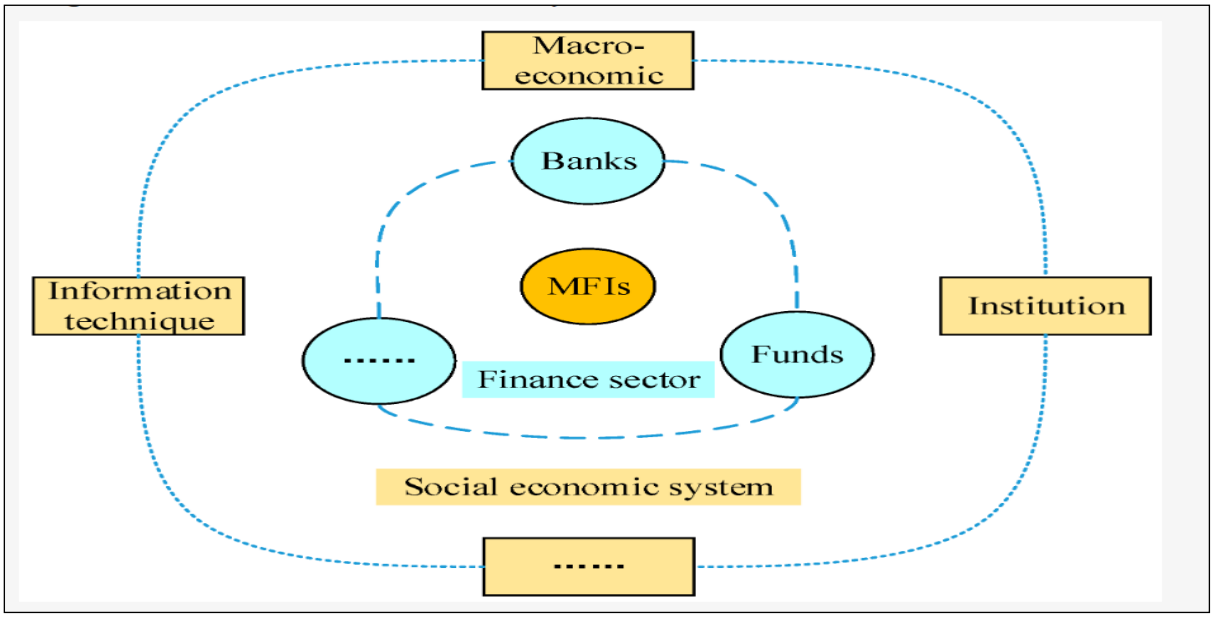

Figure 2: MFB/MFI and Social Economic System.

Source: Xu et al., (2019:3)

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

a. The Sustainability of MFBs

Understanding the characteristics of MFB is fundamental before one examines the sustainability of this type of institution. Low-cost goods and services, simple opening procedures, accessible financial instruments, and regulated return guarantees define MFB (Garcia-Perez, Fernandez-Izquierdo and Munoz-Torres 2020). MFBs aim to provide the most vulnerable people with the resources they need to meet necessities, deal with personal problems, or grow a small business, among other things (Garcia-Perez et al., 2020). Given the characteristics of MFBs, the notion of their sustainability differs slightly from that of sustainability in general. From a comprehensive standpoint, sustainability is viewed as a balance between the financial, environmental, social, and governance (FESG) dimensions, underlining the significance of the interrelationship among the four dimensions in the short- and long-term (Garcia-Perez et al., 2020).

A slightly different approach emphasises the financial (economic) and social sustainability pillars in the notion of sustainability for MFBs. The importance of financial sustainability is highlighted by MFBs' increased financial independence and decreased reliance on donor financing. Focus is placed on social outreach in social sustainability. Sustainable MFB is described by Navajas, Schreiner, Meyer, Gonzalez-Vega, and Rodriguez-Meza (2020) as the continuity of ongoing financial services to "unbankable poor and small companies". In this regard, it is essential to note that sustainable MFBs maintain outreach and profitability simultaneously. The social impact of MFBs is related to social sustainability (Xu et al., 2019). More studies have recently focused on the environmental sustainability of MFBs, while examining the green environment performance of MFBs, in addition to social and financial sustainability (Nawaz, Selva and Savino, 2016). To achieve social and environmental sustainability, an MFB must be financially sustainable. Garcia-Perez et al. (2020) considered economic, social, and environmental factors when analysing the sustainability concept of MFBs. Below is figure 3, which depicts the three essential aspects when defining the sustainability of MFB.

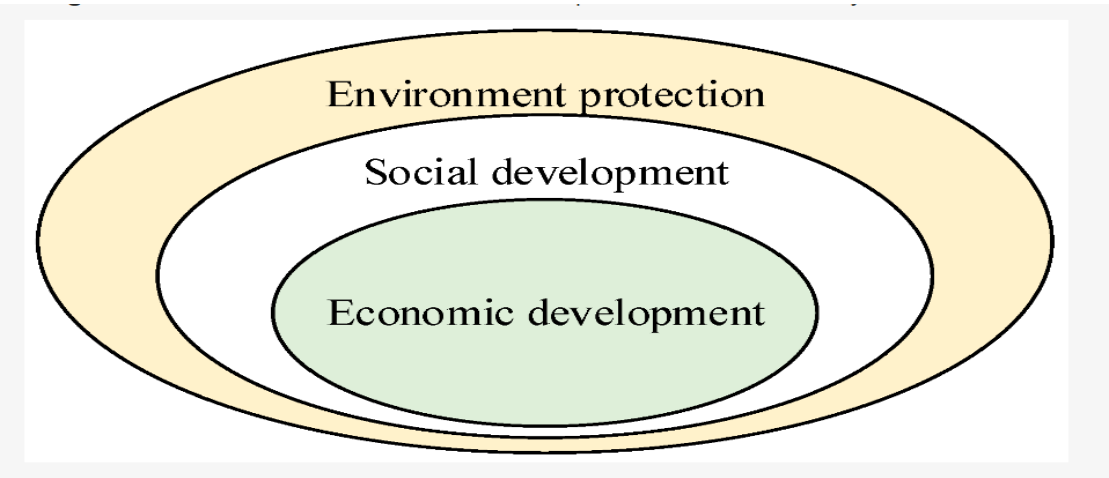

Figure 3: Three interrelated sustainability definition domains or pillars

Source: Xu et al., (2019:4)

For this study, the sustainability of MFB is defined as the capacity of a microfinance provider to cover all of its expenses and to continue offering and expanding financial services to the underprivileged. The sustainability of MFB is operationalised by two items, namely continued operation and expansion of operations by the MFB. Financial sustainability in the microfinance industry suggests that sector revenue should exceed service costs.

II. METHODS

This study adopted a positivistic paradigm to determine the effect of cyber security on business sustainability in Nigerian MFBs. The target population of this research is twenty-five (25) listed microfinance firms on the Nigeria Stock exchange as of December 2021 (NSE Facts book, 2020). A simple random sampling technique was utilised to select Nigeria's three most valued microfinance banks in terms of high capitalisation, national coverage, and covered by Nigeria Deposit Insurance Corporation (NDIC). KUDA, LAPO, and Accion Microfinance banks were selected based on these conditions.

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

Table 1: Sample of selected MFBs in Nigeria

SS/N	*Names of MFBs*	*Number of employees (senior, medium and junior)*
1	*KUDA Microfinance Bank*	*114*
2	*LAPO Microfinance Bank*	*108*
3	*Accion Microfinance Bank*	*93*
	Total	*315*

Source: Field Survey, 2022

The population size was used in this research as the sample. The decision to adopt a census was adopted in this study because the size of the population is manageable. Additionally, the senior, medium and junior employees of the sampled MFBs were considered in the study because cyber security is always considered everybody's business.

Data were collected from the (senior, medium and junior) employees of the sampled MFBs using a questionnaire with a five (5) point Likert scale. A total of 305 respondents filled and returned their questionnaires used for the analysis, while ten respondents could not return theirs.

To maintain the instrument's validity, the first draft of the questionnaire went through content and face confirmation. The initial draft of the instrument was given to experts in the banking sector in Abuja, Nigeria, as well as other Security and Forensic experts in Abuja (identities withheld for security reasons). These experts were employed to examine the items in the instrument and expressed their views on the suitability and clarity of the statement in the questionnaire. The final copy was modified based on the expert suggestions and opinions. The questionnaire underwent a reliability test using Cronbach's Alpha. The reliability of the questionnaire was found not to be less than the Alpha value of 0.7, as Nunnally (1978) approved.

Table 2: Summary of the Reliability Measurement (Cronbach's Alpha)

Questionnaire Variables	*Cronbach's Alpha*
Cyber Security	*0.795*
Microfinance bank Sustainability	*0.781*

Source: SPSS-25, 2022

Table 2 reveals that the reliability of the variables has an Alpha value above 0.70, which implies that they are reliable.

Multiple regression analysis is used to analyse the collected data. Multiple regression analysis was used to determine the degree of effect of the independent variables on the dependent variable in the study. Below is the model specification for this study:

Y= $\alpha + \beta_1 x$.....1,

Y=dependent variable, α =intercept,

β_1 = coefficient, X is the independent variable.

SMFBs = $\alpha + \beta_1$ CS+ μ .....2.

Where: SMFBs = Sustainability Microfinance Banks.

β = coefficient,

α =intercept,

μ = error term.

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

III. RESULTS AND DISCUSSION

The three listed and some of the most valuable MFBs in Nigeria were studied using Pearson's correlation coefficient and multiple regression analysis to determine the relationship between cyber security and the sustainability of MFBs. Pearson's correlation coefficient was used to determine the relationship between cyber security and MFB sustainability. The contribution of each cybersecurity element on MFBs sustainability was also determined using multiple regression analysis. As a result, table 3 demonstrates the relationship between these variables.

Table 3: Pearson's correlation coefficient between cyber security and business sustainability

		Cyber-security	*Business sustainability*
Cyber-security	*Pearson's Correlation*	*1*	*531***
	Sig. (2-tailed)		*.001*
	N	*305*	*305*
Business sustainability	*Pearson's Correlation*	*531***	*1*
	Sig. (2-tailed)	*.001*	
	N	*305*	*305*

**. Correlation is significant at the 0.01 level (2-tailed).

The relationship between cyber security and MFBs sustainability is correlative (r = 0.531, p 0.05) and is shown in Table 3. Cybersecurity and the dependent variable are significantly and positively related, according to the table of correlation coefficients (business sustainability). With a correlation coefficient of 0.531 or 53.1%, the p-value is less than 0.05. The null hypothesis was rejected at this significance level, indicating a significant and favourable relationship between Nigerian MFB's sustainability and cyber security (confidentiality, integrity, and availability).

However, the relationship between the two variables is equally strong and favourable in addition to being significant. A multiple regression analysis was used to conduct additional tests after determining a relationship between cyber security and business sustainability. These tests sought to determine the individual contributions of each cyber security component to the sustainability of MFBs in Nigeria. The findings of the exploratory factor analysis (EFA), which determines the factor loading of each cyber security attribute, are shown in Table 4.

Table 4: Exploratory factor analysis of the attributes of cyber security

Item	*Mean*	*SD*	*Factor loading*	*Item total correlation*
Cyber security				
Factor 1				
Data confidentiality	*4.71*	*1.231*	*.771*	*.573*
Data integrity	*4.12*	*0.927*	*.628*	*.524*
Data availability	*3.92*	*1.524*	*.659*	*.512*

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

KMO = .731; X2 = 542.113; DF= 4; P < .002; Cronbach's α = .672; Percentage of variance explained = 63.76%.

This study assessed the internal consistency of the many measurements employed in the research construct using reliability. Using IBM SPSS statistics version 26, the internal consistency of the component factors and items from the EFA test was examined. The Cronbach's alpha coefficients are given as data: confidentiality (0.678), data integrity (0.563) and data availability (0.724). A factor consisting of MFBs sustainability produced an internal consistency of 0.685. Since Cronbach's alpha coefficients were over 0.600, no factor was eliminated from the measurement model. The cyber security components of this study were analysed using the multiple regression analysis/model measurement shown in Table 5 based on the outcomes of the EFA. The result combines the model summary, the ANOVA, and the coefficients in table 5 to give a clear and comprehensive picture.

Table 5: Cyber-security as predictors of business sustainability

	R	*R2*	*Adjusted R2*	*F*	*Beta*	*T*	*Sig*
	798a	*0.638*	*0.513*	*19.832*	----	----	*.000b*
Data Confidentiality					*161*	*.531*	*.000*
Data integrity					*-.282*	*-1.853*	*.002*
Data availability					*.311*	*2.982*	*.001*
(Constant)					---	*2.715*	*.007*

a. Dependent Variable: business sustainability
b. Predictors: (Constant) confidentiality, integrity, availability

Table 5 reveals that the regression model's R square is 0.638, and its adjusted R square is 0.513. In other words, 51.3% of the variations in the MFBs' ability to sustain their businesses in Nigeria may be predicted by the model (cybersecurity). This is significant at the level of 0.05, indicating a significant correlation between the independent variables of cyber-security features and the dependent variable, namely business sustainability. These findings are consistent with the alternative hypothesis that cyber security affects Nigeria's MFBs' capacity to sustain their businesses. Notably, the standardised Beta and the corresponding P-values for *data confidentiality* (β = -0.161, p<0.000), *data integrity* (β = -0.282, p<0.002), *data availability* (β = 0.311, p<0.001), show that data availability made the largest contribution to the model, followed by data confidentiality and data integrity which pose a negative sign. In light of these findings, data accessibility and confidentiality work together to forecast the sustainability of MFBs in Nigeria.

A. Discussion of Findings

The findings of this study reveal that employees of MFBs uphold the view that cyber security has a positive and significant effect on the sustainability of MFBs in Nigeria. From the viewpoint of employees in this study, data availability makes the largest contribution to the business sustainability of MFBs in Nigeria, followed by data confidentiality and data integrity. While digital financial service provision by MFBs is conceived as more efficient especially because of the ability to deliver at significant scale with significant reduction in delivery costs, a bigger opportunity for business sustainability is missed when service and data is inaccessible to authorised users and customers. This study underscores that the sustainability of MFBs is easily jeopardised by the lack of availability of data and services when required by internal and external stakeholders (e.g. employees and customers) in many ways (e.g. system access error, power outage, internet problems). Drawing from the market rather than organisational perspective, Kolade (2022) asserts that users of financial services by banks in Nigeria face availability threats, such as the collapse of hardware or software, power failure, natural circumstances beyond one's control, and human error. One of the most well-known attacks that jeopardise the availability of MFBs is the denial-of-service (DoD), or when financial service is knowingly and maliciously tarnished, or the system becomes completely inaccessible.

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

Consistent and timely availability of service and data with easy accessibility by authorized customers and users is a strategic component of cyber security which enhances the supply side and sustainability of micro banking business (Kolade, 2022). Market penetration and growth in a micro banking market are easy when customers trust the digital finance services and its accessibility. Garcia-Perez et al. (2020) uphold that the goal of MFBs is to provide the most vulnerable people in society with the resources they need to meet necessities, deal with personal problems, or grow a small business, among other things. Kolade (2022) is cogent that digital finance by MFB is widely regarded as one of the most viable, effective, and result-oriented tools to empower poor people and increase their financial inclusion. However, MFBs can only scale up their activities and maximise coverage of financial services if they effectively leverage technological advantages, especially Information and Communication Technology (ICTs) to meet customer and market demands (Chang & Coppel, 2020). Succinctly, the social and financial dimension of the sustainability of MFBs may not be achieved and sustained if the service is unavailable and not resilient in the face of challenges such as power outage. Unauthorised access to financial systems undermines not only availability of service to user, but also the confidentiality, and integrity of service and data for authorised users (Perwej et al., 2021).

The finding that cybersecurity positively affects the sustainability of MFB also invokes questions on the strategies used by various stakeholders, especially customers of financial services and MFI, to deal with different forms of cyber risks in the environment. A study by Ugwuja and Adesope (2021) revealed a variety of cybersecurity measures used mainly by female heads in Nigeria. These include avoiding isolated ATMs, not going to the ATM during late hours, and ignoring and deleting emails and text messages requesting online banking information. Female heads of households stopped using birthdates, addresses, and other words or numbers in their passwords, which makes it easier for attackers to guess and not use the same password for all their different bank accounts. These behaviours indicate that the individual customer has a significant role in achieving cyber security. It is prudent that MFBs understand not only the impact of cyber security on the supply side, but also the demand side of digital financial service. For example, customers may lose confidence and trust in the financial service, and also suffer a financial and psychological harm if they become a victim to a scam or experiencing system access errors (Ugwuja & Adesope, 2021). More importantly, it is arguable that the majority of the customers of MFBs do not have digital literacy but also lack adequate technical competence and familiarity to mitigate cyber crimes. Customers of MFBs are also more likely to use devices and channels not designed to offer the security needed for a financial transaction (e.g., USSD technology) (Anoke et al., 2021). Thus safety, security and resilience are key building blocks for availability as part of cyber security to build customer trust to navigate the cyberspace. Customers are potential victims of cyber-attacks and external beneficiaries whenever there is strong cybersecurity in a MFB.

From the business and cybersecurity perspectives of sustainable MFBs, it is cardinal to ensure ongoing customer education on cyber risks and promote behaviours that enhance cyber security at the individual level when operating in cyberspace. Additionally, MFBs need to continuously monitor e-banking channels (such as cards, point-of-sale systems, ATMs, and other channels) to ensure the availability of service and integrity of data and to build stakeholder trust in digital financial transactions.

This study has illuminated that data availability, confidentiality and integrity complement each other as parts of CIA triad in MFBs. MFBs use techniques which govern permission to access data and encryption so that data availability is only to authorised parties. Arguably, the sustainability of MFBs can be negatively affected if stakeholders hold the belief or perception of compromised data integrity. In a nutshell, users of financial services may be discouraged from using financial services if they suspect that data will be corrupted or changed before, during, or after submission (Navajas et al., 2020). Cyber hygiene programmes for the users of financial services and the public are essential to ensure data integrity is not undermined by corruption in the banking sector and Nigerian society. Any alteration of data for selfish reasons by staff negatively affects the MFB's sustainability and its image. In devising strategies to enhance cybersecurity, MFBs need to be holistic (e.g. focus on each aspect of CIA, external and internal sources of cybersecurity threats). A study by Omodunbi, Odiase, Olaniyan, and Essan (2016) revealed that Nigeria's cyber security could prevent cybercrime from inside and outside an organisation's cyber environment. Financial institutions are forced to invest heavily in strengthening and innovating their cybersecurity defences as cybercriminals are becoming more sophisticated in their attack methods (Aragba-Akpore, 2022). Generally, cyber-attackers do not only have a thorough understanding of the banking system's inner workings and crimes that affect computer networks and devices directly but also crimes facilitated by computer networks or devices (Aragba-Akpore,2022).

One critical aspect of enhancing cybersecurity relates to the human resource capacity of technicians and IT staff to detect and respond to the threats of cyber attackers. Aragba-Akpore (2022) asserts that without ongoing training, the human element is considered inadequate to deal with the ever-changing trends of cybercrimes in many MFBs in Nigeria. Continuous training of IT officers, especially with emerging trends of attacks and counter-measures to defuse attacks which undermine the sustainability of MFBs, is very important in MFBs. As the nature and complexity of cybersecurity change, MFBs are implored to ensure that risk management strategy is regularly

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

reviewed, revised, and strengthened to address new difficulties as they introduce more innovative financial products and services. A study by Alawonde (2020), which focused on six chief information security officers from six financial institutions, illuminated four strategies used by financial institutions in Nigeria to prevent cyber exploitations. First, the study revealed strategies depicting policies, processes, and procedures (Alawonde, 2020). These strategies cover information and IT tools and services to ensure the ongoing security of information assets. In MFBs, information security risk management is critical as it involves determining an organisation's information security risks, identifying risk tolerance levels, and deploying controls to ensure that information security risks are at acceptable levels.

Second, financial institutions also use a variety of people strategies to enhance cybersecurity (Alawonde, 2020). These strategies cover the human element that financial institutions use to avoid cyber exploitations. Training of customers and system users to understand acceptable behaviour to prevent cyber exploitations of confidentiality, integrity and availability of information assets) is vital in any organisation. Even where other controls are in place, the human element can allow evasion of controls. While people-related strategies address potential human errors that lead to a breach of information security, they also seek to forestall insider-related threats. Multi-stakeholder orientation acknowledges that there are diverse key actors in achieving cyber security while human-centred cybersecurity relates to the interaction between the human and the data (e.g. malicious insider, an accidental insider, or a compromised insider).

Third, an effective consumer protection framework (e.g. dealing with complaints, consumer education and financial literacy) and promotion of consumer confidence in the financial system are essential to ensure an appropriate level of protection in terms of confidentiality, integrity, and availability of information assets (Alawonde, 2020). Lastly, technology-related strategies and solutions affect the network, applications, databases, operating systems, endpoint, user devices and other technology tools within the IT environment of organisations.

Kolade (2022) acknowledges that in Nigeria, there are challenges to enhancing consumer trust and security in the digital environment. For example, Nigeria's central bank digital currency, known as the eNaira, suddenly vanished from Google Play, further raising skepticism among users. To build customer trust, MFBs must deploy mechanisms to ensure their risk management process and information security management tasks are holistic and cover the universe of information security (e.g. awareness, continuous capacity building and monitoring). Technology-related aspects of cybersecurity have a systemic risk arising from the interconnection between various actors and elements within a system and network of financial systems in the cyber ecosystem. At the societal level, MFBs' fighting cyber-crimes through cyber security can yield better results by lobbying the government to enhance the closure of "yahoo yahoo" academies enrolling youth to train in cybercriminal activities, and the support of the Nigerian youth to re-direct their energy and intellectual power in gainful, legal and productive work (Aragba-Akpore,2022). MFBs require a more supportive ecosystem (e.g. programmes to enhance digital financial literacy, robust anti-cybercrime laws, youth economic empowerment) to be able to undermine and manage the cyber risks associated with digital financial services against the backdrop of aggressive recruitment of youth into cybercrimes as a rewarding activity. MFBs are cautioned not to overlook the human elements and multi-stakeholder orientation by simply focusing on adopting new technologies, processes, and cybersecurity standards.

B. Three Managerial Implications and Areas of Future Research

Three implications of this study relate to a paradigm shift, pursuit of integrative and collaborative cyber security strategy and re-conceptualisation of cybersecurity for research in future.

1. Shift to pronounce human-centric cybersecurity

Firstly, there is a compelling need for MFBs to shift to human-centric cybersecurity from the prevailing paradigm of cybersecurity, which is construed as exclusively the domain of IT experts and focused on technology. As business sustainability involves business, technology and people, MFBs are implored to pronounce human-centric cybersecurity, which works in tandem with cybersecurity defence technology to achieve optimal efficacy and customer trust. This re-orientation implies clarity that cyber security is not just about cybersecurity technology alone, as there is a human element capable of enabling or impeding cyber security as well as the social and financial dimension of the sustainability of MFBs in Nigeria. As such, it is prudent for MFBs to adopt a multi-stakeholder approach in implementing cybersecurity strategies targeting financial services if they are to ensure that cybersecurity positively influences the sustainability of MFBs in Nigeria.

2. Integrative pursuit of cybersecurity strategy

Secondly, the pursuit of an integrative cybersecurity strategy by MFBs is salient to deal with systemic risks arising from technology and interconnection between the various elements of their systems and sub-systems involved in the service chain for financial services. The integrative approach implies that MFIs integrate technology, information risk management processes, and human elements within the organisation to achieve data availability, confidentiality, and integrity goals. Collaborative implementation of public communication as a tool

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

must educate the public and target financial services, products and their usage in ways which build trust among various stakeholders to engage in a secure online space.

3. Process, outcome and stakeholder centricity

Lastly, future research to enrich the complexity of our understanding of cybersecurity needs to move beyond the restricted notion of the CIA triad. Re-conceptualising cybersecurity in a way that elaborates both the process and outcomes of how the tech, human and business aspects of cybersecurity integrate into a whole can aid our understanding of cybersecurity from a business and strategic viewpoint. More importantly, it is imperative that the re-conceptualisation of cyber security takes cognisance of multi-level interactions of individual and organisational level strategies in the cyber environment when using and providing digital financial services. Mindful that cybersecurity is the task of every individual in a MFB, scholars are implored to re-conceptualise the phenomenon of cybersecurity in ways which embrace stakeholder-centricity. This aspect in re-conceptualising cyber security is pivotal in situating cyber security at the intersection of the individual as an attacker, customer or insider user and collective responsibility within a MFB while recognising the role of the industry and society.

One of the limitations of this study is the exclusive and inward focus on employee perspectives on cybersecurity and business sustainability of MFBs. While the study used a sample of diverse employees at different levels in the organisation, it is clear that the focus has exclusively been on views of employees to understand business sustainability. As cyber risks affect both internal and external stakeholders, it is critical that future research on cybersecurity and its effect on business sustainability is more inclusive to embrace at least the customer's perspectives. This resonate with the view that customers are a source of revenue critical for business sustainability in the business arena. Employee views on cybersecurity and business sustainability are key, but needs to be complemented with customer perspectives in future research if we are to enrich our understanding of the effect of cybersecurity on business sustainability in MFBs but also any other type business.

V. CONCLUSION

The study has investigated the effect of cyber security on MFBs' sustainability in Nigeria. The results reveal that employees of MFBs in Nigeria uphold the view that cyber security positively and significantly affects the business sustainability of their organisations. From the employee perspective, cyber security is a critical strategy for the sustainability of MFBs, which calls for attention to data availability to authorised internal and external stakeholders when required in ways that ensure data confidentiality and data integrity in Nigeria. It is pivotal for MFBs to ensure that risk management strategy is regularly reviewed, revised, and strengthened to address new difficulties brought on by introducing innovative financial products and services.

Overall, this study is a critical step in reinforcing that digital financial systems and financial services require cyber security as a central feature which impacts internal and external stakeholder trust in digital financial services in cyberspace and the business sustainability of MFBs in Nigeria. While the CIA triad remains insightful in unravelling cybersecurity, it is more prudent for future researchers to adopt a more integrative and collaborative approach that captures the multi-dimensional, processual and human aspects of cybersecurity and link these to businesses sustainability.

REFERENCES

Alawonde, K (2020). Tailored Information Security Strategies for Financial Services Companies in Nigeria, Doctoral Study Submitted in Partial Fulfillment of the Requirements for the Degree of Doctor of Information Technology, Walden University, College of Management and Technology

Anoke, A.F. (2019). Growth strategies and performance of listed insurances firms in Nigeria; *Journal of Accounting, Finance and Development, 2(1),* 49-60

Anoke, A.F., Ndubuisi-Okolo, P.U. (2022). Entrepreneurial mind-set among Nigeria University Students: A study of Ebonyi State University's entrepreneurship Centre, Abakaliki. *Asian Journal of Economics, Business and Accounting 22*(5):24-33

Anoke, A.F., Nzewi, H.N., Agagbo, O.C., and Onu, A.N. (2021). Micro insurance services and growth of women entrepreneurs in Onitsha, Anambra State, Nigeri,. *International Journal of Innovative Science and Research Technology, 6(8):* 507-513.

Aragba-Akpore, S (2022). Digital literacy and rising cybercrimes, THISDAY Newspaper. https://www.thisdaylive.com/index.php/2022/06/01/digital-literacy-and-rising-cyber- crimes

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

Ashrafi. M, Acciaro. M, Walker. T, Magnan. G & Adams. M. 2019.Corporate sustainability in Canadian and US maritime ports. *Journal of Cleaner Production,* 386-397.

Catal C, Ozcan A, Donmez E, Kasif A. (2022). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Educ Inf Technol (Dordr). 5:1-23.

Chang,L.Y and N. Coppel, N (2020). Building cyber security awareness in a developing country: lessons from Myanmar. Computers & Security, 97, 101959, 2020

Duncan, B and Westerlund, M(2022).Cost-Effective Permanent Audit Trails for Securing SME Systems when Adopting Mobile Technologies. Conference: IARIA Cloud Computing 2022: The Fourteenth International Conference on Cloud Computing, GRIDs, and Virtualization, Barcelona, Spain

Ebelogu, C., Ojo, S., Andeh C , and Agu E.(2019). Cybercrime, its Adherent Negative Effects on Nigerian Youths and the Society at Large: Possible Solutions. *International Journal of Advances in Scientific Research and Eng*ineering. 5,12,154-166.

Fashagba, M.O., (2018). The impact of insurance on the economic growth in Nigeria; Afro Asian *Journal of Social Science, 9(1),3-14.*

Garcia-Perez, I., Fernandez-Izquierdo, M.A. and Munoz-Torres, M.J (2020). Microfinance institutions fostering sustainable development. *Sustainability*, 12, 2682, 1-22.

GCI (2020). Global Cybersecurity Index

Miracle, A., Armah, E.D., Mohammed, N & Sackey-Sam, S (2021).The antithetical effect of cybercrime on Small Medium Enterprise: Public assessment. *International Journal of Multidisciplinary Studies and Innovative Research*, 7, 479-481

Kolade, E(2022). Cybersecurity in Nigeria's Financial Industry: Enhancing Consumer Trust and Security, Carnegie Endowment for International Peace, https://carnegieendowment.org/2022/05/13/cybersecurity-in-nigeria-s-financial-industry-enhancing-consumer-trust-and-security-pub-87123

Morgan, S. (2020). Cyber-crime to cost the world about ten point five (10.5) trillion dollars annually by 2025. Cyber warfare in the C-suit

Navajas, S., Schreiner, M. Meyer, R.L. Gonzalez-vega, C. Rodriguez-meza, J. (2020). Micro credit and the Poorest of the Poor: Theory and Evidence from Bolivia. *World Development*, 28, 333–346.

Nawaz,S., Selva, V.D. and Mario, M (2016). Extensive Literature Review to Investigate the Dimensions of Business Sustainability 22, 3, 273-302.

Nunnally, J. C (1987). Pyschomatic Theory Theory (2nd edition) New York, McGraw-Hill

NSE Fact Book (2020). Nigeria Stock Exchange FactBook 2020

Okonkwo, I.V. and Okereke, D.C. (2019). Development and innovation in Nigerian Insurance industry:2010-2018. *International Journal of Research in Business, Economics and Management.3 (1), 105-121.*

Omodunbi, B.A., Odiase, P.O., Olaniyan, D.M., & Esan, A.O. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention. *Fuoye Journal of Engineering and Technology; 1(1), 37-42.*

Perez, B., Bacotti, ., Peteri, K., & Vollmer, T. (2020). An extension of common used toilet - training procedures to children with autism spectrum disorder. *Journal of applied Behaviour Analysis 53(3)*

Perwej, Y., Abbas, S.M., Dixit, J.P., Akhtar, A & Jaiswal, AK (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management,* 9 (12),669-710.

Prakash,M(2022). CIA Triad in Cyber Security: Definition, Examples, Importance. https://www.knowledgehut.com/blog/security/cia-in-cyber-security

Popescul, D. & Cuza, A.I (2011). The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation., Proceedings of The 16th International Business Information Management Association Conference (Innovation and Knowledge Management, A Global Competitive Advantage), June 29-30, Kuala Lumpur, Malaysia, 1338-1345

Seemma, P.S., Nandhini, S., & Sowmiya,M. (2018). Overview of cyber security; International *Journal of Advance Research in Computer and Communication Engineering,7(11), 2-5.*

Uddin, M. H., Ali, M.H. & Hassan, M.K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature, *Risk Management*, 22(4), 239-309.

Ugwuja, V.C & Adesope, O.M (2021). Cyber risks in microfinance digitization: exposures and preventions among female headed farm households in southern Nigeria. *European Journal of Agriculture and Food Sciences,* 3, 3, 62 -68.

WECD (1987) World Commission on Environment and Development

Xu, W.; Fu, H.; Liu, H. (2019). Evaluating the Sustainability of Microfinance Institutions Considering Macro-Environmental Factors: A Cross-Country Study. *Sustainability,11*, 5947, 1-22.

ISSN : 2597-4785 (ONLINE)
ISSN : 2597-4750 (PRINTED)

Yakubu, A.M. (2017). Cyber security issues in Nigeria and challenges. *International Journal of Advanced Research in Computer Science and Software Engineering;* 7(4), 315-321.