Int Journal of Social Sciences Management and Entrepreneurship 8(3): 1037-1051 2024

ISSN 2411-7323

www.sagepublishers.com

ZERO TRUST MATURITY MODEL AND CYBER RESILIENCE IN MOBILE MONEY PROVIDERS IN NAIROBI CITY COUNTY, KENYA

[1] Musyoka Samuel Muthoka, [2] Dr. Mose Thomas, PhD

[1] Master of Science (ICT Management) Jomo Kenyatta University of Agriculture and Technology

[2] Lecturer, Jomo Kenyatta University of Agriculture and Technology

ABSTRACT

Mobile money services have revolutionized the payment system in Kenya, bringing significant benefits to both the economy and its citizens. However, as the industry has grown and evolved, it has also faced significant cybersecurity challenges that have resulted in financial losses for mobile money providers. Despite investing heavily in security controls and countermeasures, the industry has struggled to keep up with emerging cyber threats. To combat these challenges, mobile money providers have implemented a range of security strategies, from traditional measures like encryption mechanisms and user authentication to more innovative approaches such as API security and deployment of security operations centers. These efforts have been coupled with education and awareness campaigns to sensitize all stakeholders to the risks of cybercrime. Despite these efforts, cyber threats continue to evolve due to emerging technologies taking shape, and new strategies are needed to address them effectively. Therefore, it is essential to continue developing innovative approaches in cybersecurity that go beyond technology and devices to ensure provision of secure and sustainable mobile money services to consumers. By doing so, organizations can build trust in their system and continue reaping the benefits of these transformative and adaptive security technologies. Ensuring cyber resilience is crucial across all aspects of an organization, encompassing people, processes, and technology. This is critical for mobile money service providers because trust and confidence in provision of their services are vital in ensuring a safe and secure environment. To achieve this, a zero trust mature security model can significantly influence these providers. By implementing the principles behind this model, they can create a more secure environment, gain competitive advantage, and offer better measures against cyberattacks and fraud. Therefore, this study aimed to examine the influence of zero trust mature model principles on mobile money providers in their pursuit of cyber resilience. Identity access management was shown to substantially enhance cyber resilience by securing user authentication and access controls. Additionally, cybersecurity operations management were found to positively influence cyber resilience, emphasizing the importance of proactive threat detection, incident response, and robust data protection measures. Collectively, these results highlight the need for a comprehensive approach to cybersecurity, integrating multiple strategies to strengthen mobile money platforms against evolving threats.

Key Words: Zero Trust Maturity Model, Cyber Resilience, Mobile Money Providers, Identity Access Management, Cybersecurity Operations Management

Background of the Study

As a global pioneer of mobile money, Kenya has made significant strides in providing financial inclusion to the underbanked population over the years. However, much remains to be done to unlock the promise of truly inclusive secured mobile money services and address the real-world cyber security challenges faced by the providers of these services (Mobile for Development, 2021). A report by GSMA (2024) indicated that global registered mobile money accounts stood at $1.75 billion as of 2023 which was an increase of 12% from the previous year in 2022.The value of mobile money transactions rose to $1.4 trillion over the period of 2023 a 14% increase compared to the previous year in 2022.This exponential growth has been attributed to the continuous maturity of the industry while depicting mobile money services as the driving force to emerging economies globally. A similar report by GSMA (2019) estimated that the cost of cybercrime in the mobile money industry in Kenya in 2018 was $295 million. According to a survey by Blackmon and Mazer (2021), 8.4% of mobile money users in Kenya have reported lost funds on their mobile money account and 70% of these cases were due to third-party phone or SMS related fraud in 2021.

With these statistics, it is worthwhile to note mobile money services are delivered through a large and complex ecosystem multiplying the risk of financial fraud (Mobile for Development, 2021). As a result, advanced cybersecurity approaches are vital in driving mobile money adoption, its use and cybersecurity operations management (Awanis and Lowe, 2022). Continued efforts to document and standardize effective financial fraud and risk management approaches have attempted to accelerate the growth and development of mobile money services (Ambore and Richardson, 2017).There is an obligation by mobile money providers to build in external controls over and above the traditional internal perimeter controls which they cannot rely solely on user behaviour and safe practices (Ajufo, 2022).For instance, numerous global mobile money services best practices include caps on the number and size of mobile payment transactions and these limits are designed to lessen the risk of systemic failure or contagion but can also reduce the potential losses from financial fraud. Separately, technical checks for other financial institutions to adopt and implement with relative ease are important. To this effect, some payment switch providers have developed open-source fraud management and anti-money laundering systems. Such accessible and interoperable systems are well-suited for a diverse mobile money environment (Ajufo, 2022).

The growing sophistication, frequency, and severity of financial fraud targeting mobile money providers highlight their inevitability and the impossibility of completely protecting the integrity of mobile money environments. Cyber-resilience offers an attractive and holistic complementary alternative to the existing cybersecurity paradigm. Dupont (2019) defines cyber-resilience as the capacity to withstand, recover from, and adapt to the external shocks caused by cyber risks in an organization. To achieve cyber resilience, various mobile money providers have been adopting conventional information security models around CIA (Confidentiality, Integrity, and Availability) triad that have mostly catered for external threats, and little has been done on the internal threats (Kaur and Lashkari , 2021). This therefore necessitates the mobile money industry to adopt an information security model that provides an all-round threat protection, with effective security governance and business continuity. A shift towards a business imperative with the implementation of a zero trust mature model was ideal to address this never-ending predicament and ensure that these organizations strive towards a cyber-resilient environment.

A zero trust mature model is defined as an information security model that denies access to applications, network, or data by default by eliminating implicit trust and continuously validating every stage of a digital interaction rooted in the principle of ‘never trust, always verify’(Cody , 2022).Threat prevention is achieved by only granting access to applications, networks and data utilizing policies informed by continuous, contextual, risk-based verification

across users and their associated devices. However, it is important to note that zero trust is a cybersecurity paradigm where security should be evaluated and used continually which indicates that trust is not granted implicitly but must be continually evaluated (Presence Secure, 2024). According to Gartner, only 1% of large enterprises have a mature and measurable zero trust program in place today and only 10% will achieve that by 2026 (Robinson, 2023).

Statement of the Problem

The exponential growth in the industry over the years is directly proportional to cybercrimes and financial fraud which mobile money services have also rapidly become a conduit for fraud and other criminal activities (Buku & Mazer, 2017). The mobile money industry faces a diverse range of security challenges due to the dynamic digital landscape and emerging technologies such as 5G networks , robotics, quantum computing, internet of things (IoT) that have catapulted cyberattacks. These challenges are multifaceted, interconnected, and continually evolving, necessitating robust and adaptive security measures. The prevalence of cyber threats, including sophisticated malware, ransomware attacks, phishing, and social engineering campaigns, has escalated in recent years, demanding advanced cybersecurity strategies to combat the complexity and variety of these attacks (Aslan & Aktuğ, 2023).

A study by Sharif & Mohammed (2022) reveals that global losses from cybercrime are projected to reach a staggering $10.5 trillion annually by the year 2025, emphasizing the need for enhanced and different approaches towards cybersecurity. As mobile money services gain widespread adoption, there is growing risk of cybercrime, identity fraud, and SIM swapping. This has prompted mobile money providers to prioritize the protection of their services and the sensitive customer data known as "Know Your Customer" (KYC) by implementing robust security measures around these assets (Hoverman, 2018). All the inbound and outbound data in these organizations is commonly channeled via a single internet gateway by internet providers or on physical devices. Despite increased coverage of security breaches, many organizations are still grappling to protect their networks using traditional firewalls and other outdated security solutions (Hoverman, 2018). Traditional cyber security models focus on blocking mechanisms in contrast to emerging security models that focus on thorough and continuous verification rather than blocking (Sarkar & Choudhary, 2022).

Another study conducted by Wambugu GSMA (2024) focused on the dynamics of various fraud schemes and identified impersonation schemes as the most prevalent in mobile money industry. Identity fraud ranked as the highest mobile money fraud scheme at 90.38%, followed by social engineering schemes at 88.46%. Insider fraud ranked third at 86.54% while another, impersonation scheme and SIM swap fraud ranked fourth at 78.85%. Cyber fraud ranked fifth at 59.62%. Further to this, a Central Bank of Kenya (2023) report in 2023 indicated that 6.1% of mobile banking users and 25.9% of mobile money users had lost money through cybercrime in Kenya. Other cyber security risks in the industry have been attributed to money laundering and terrorism financing. In essence, mobile money providers should remain vigilant in monitoring activities of their customers to avoid promoting unlicensed activities such as online forex trading and processing of transactions associated with digital assets such as cryptocurrencies unless verified accordingly by the industry regulator (Central Bank of Kenya, 2023). Nevertheless, mobile money operators in Kenya have put in place measures to ensure the security of all transactions, including end to end data encryption mechanisms, secure authentication protocols, network and firewall fences, data protection measures etc. Additionally, the industry regulator, the Central Bank of Kenya conducts regular audits to ensure that mobile money operators comply with the set standards in cyber security data protection (Central Bank of Kenya, 2023). However, there is still a need for continuous efforts to attain cyber resilience with the improvement of cybersecurity by mobile money platforms in Kenya to protect their users and employees from any potential cyber threats. Despite the

implementation of fraud management systems, preventive measures, and detective controls by mobile money providers in Kenya, leaks are still rampant in areas such as identity theft, data protection enforcement and internal fraud, hindering the journey towards a secure and sustainable environment.

Cybersecurity risk mitigation is more than a technical problem (Mobile for Development, 2021). To overcome cybercrime in mobile money services and the accompanying threats and challenges, a holistic model is required (Mobile for Development, 2021). To ensure top-notch cyber resilience for mobile money providers, the adoption of a zero trust mature model and its underlying principles was instrumental not only in helping them stay reliable, available, and competitive, but also enable them to offer their services more securely and efficiently. In this study ,the journey towards cyber resilience in mobile money providers in Kenya was derived on zero trust mature model principles that was evaluated through performance evolution which include prevention before a cyber-attack, response during a cyber-attack, and recovery after the cyber-attack (Quanyan & Yunfei, 2023).A mature zero trust model will significantly augment the overall approach in not only combating cybercrimes and fraud but also providing a secure sustainable environment for business continuity and security governance in this industry.

Several studies have been conducted in relation to cyber resilience. A research study conducted by Kiganda (2022) on an assessment of the factors affecting cyber resilience in microfinance institutions in Kenya only focused on an analysis of factors that influenced cyber resilience in micro finance institutions in Kenya and covered management support , regulatory factors, and resources factors. Another research study conducted by Otieno (2020) was on a framework based institutional theory for cyber resiliency in the county government of Kakamega and touched primarily on threat prevention and governance within the county. Another research study by Mayunga (2019) purposed to develop a framework for measuring cyber resilience of Kenyan banks to entrench cyber resilience as a best practice. Two of these studies did not provide a model that can be adopted by organizations towards achieving cyber resilience , and the other provided an array of frameworks that banks can choose to be adopt in achieving cyber resilience. Therefore, this study recommends the implementation and application of zero trust mature model principles to improve cyber resilience in the mobile money providers to reinforce the current controls and measures that are in place.

General Objective

The study sought to establish the influence of zero trust maturity model in enhancing cyber resilience by mobile money providers in Nairobi City County in Kenya

Specific Objectives

The study was guided by the following specific objectives:

i. To establish the influence of identity access management on cyber resilience in mobile money providers in Nairobi City County in Kenya.

ii. To establish the influence of cybersecurity operations management on cyber resilience in mobile money providers in Nairobi City County in Kenya.

LITERATURE REVIEW

Theoretical Review

Compensatory Model

A compensatory model best explains a situation where a resilience factor counteracts or operates in an opposite direction to a risk factor. The resilience factor has a direct effect on the outcome, one that is independent of the effect of the risk factor. (Fergus & Zimmerman, 2005).

Based on this model, this study sought to establish that cyber resilience indicators, threat protection, business continuity management and efficient security governance have the direct effect of attaining cyber resilience in mobile money providers.

Protective Factor Model

In the protective factor model of resilience, there is an interaction between protection and risk factors, which reduces the probability of a negative outcome and moderates the effect of exposure to risk (O'Leary, 1998). This model of resilience is derived from developmental literature and systems theory. It indicates that these protective factors foster positive outcomes and healthy personality characteristics despite unfavorable or aversive life circumstances (Bonanno, 2004). The protective factors identified included emotional management skills, intrapersonal reflective skills, academic and job skills, ability to restore self-esteem, planning skills, life skills, and problem-solving skills (Ungar, 2004).This model therefore ,identifies organizational change management , effective organizational transformation and exemplary leadership skills are factors that may act as protective factors in fostering cyber resilience in mobile money providers.

Conceptual Framework

A conceptual framework is a model illustrating the interactions between independent variables, dependent variables, moderating variables, mediating variables, and control variables (Bryman, 2016). The conceptual framework in this study was founded on four independent variables namely, identity access management, cybersecurity operations management and their corresponding indicators and how these variables affected the single dependent variable, cyber resilience in mobile money providers in Nairobi City County in Kenya. The Figure 2.1 shows this interaction between these variables.

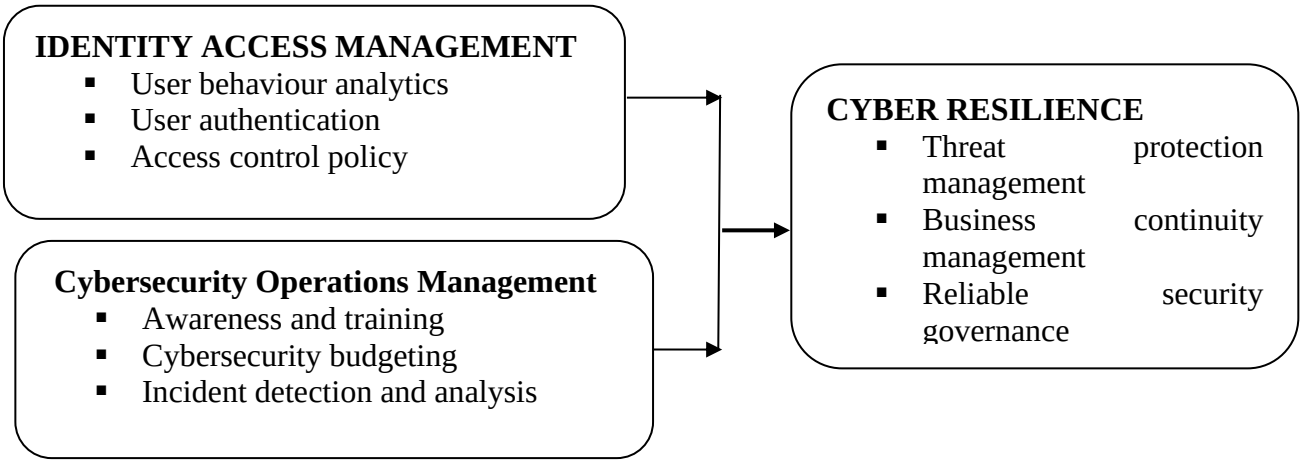

Figure 2.1: Conceptual Framework

Identity Access Management

According to Verizon, over 80% of breaches due to hacking involve lost or stolen credentials. Zero trust mitigates this risk by enforcing a policy of least-privilege access. Basically, this means users are only allowed to access resources that are essential to their role, thus preventing lateral movement in case of a breach (Enzoic, 2024).Identity Access Management (IAM) is a critical pillar of zero trust security that helps organizations control who has access to their systems and data by ensuring that only authorized users have access to the resources they need.

This confirms that IAM can be applied as a zero -trust security aspect under user access management. There are various ways in which IAM can be implemented. One way is to use IAM to implement least privilege access. Least privilege access is an essential information security principle that grants users only the minimum level of access required to perform their duties effectively (CyberArk, 2024). This best practice is widely recognized as a fundamental step in safeguarding privileged access to high-value data and assets, thereby enhancing overall cybersecurity.

Another effective approach in implementing identity and access management (IAM) is to leverage IAM for multi-factor authentication (MFA). MFA requires users to provide multiple forms of verification, such as a username and password, a security token, or a biometric scan, making it significantly harder for attackers to gain unauthorized access to systems and data (CyberArk, 2024). Furthermore, IAM can support zero trust security through the implementation of conditional access policies. These policies enable organizations to control access to resources based on various factors, including the user's location, the device they are using, and the application they are attempting to access. This ensures that only authorized individuals can access the necessary resources, even if they are trying to do so from an unusual location or device. Overall, IAM is a vital component of a robust zero trust security strategy. By properly implementing IAM, organizations can effectively protect their systems and data from unauthorized access, enhancing their overall security posture.

In cybersecurity, user behavior analytics focuses on monitoring and analyzing the activities of users within an organization’s network or applications. User behaviour analytics (UBA) analyses user data from various sources, mainly from, system logs, network logs and application logs. The primary goal of behavioral analysis is to identify and mitigate security breaches by detecting deviations from established behavior patterns. UBA also provides a holistic view of user activity across multiple systems and tools to achieve this goal of enhanced security (Katz, 2024).User behavior analytics can be a valuable addition to cybersecurity strategies, helping organizations detect and respond to potential threats more effectively which is a key factor for cyber resilience. This can enable early detection of security incidents, such as insider threats or suspicious activities, and facilitate a proactive response to mitigate risks. User behaviour analytics can be used to achieve both threat protection as a preventative aspect as well as business continuity in the event of a cyber-attack in an organization (Mathu, 2023).

User authentication is the process of verifying a person’s identity before allowing access to a system, application, or network. It requires the user to provide credentials, like username and password, before allowing it access to sensitive data or system. If the entry is validated successfully, access is granted (DesignRush, 2024).There are various user authentication factors that are used to verify a user's identity such as passwords, biometrics (fingerprint, facial recognition), security tokens, smart cards, etc. Single Sign-On (SSO) authentication method allows users to authenticate once and access multiple systems or applications without needing to log in again. Multi-factor Authentication (MFA) adds an extra layer of security by requiring users to provide multiple forms of verification before gaining access (DesignRush, 2024).To enhance the cyber resilience of user-based authentication, it is crucial to implement robust password policies. These policies may include requirements for minimum length, complexity, and uniqueness, along with restrictions on the number of attempts and the validity period. Moreover, educating formulating password policies for users is essential. Users should be informed about creating and managing passwords securely, steering clear of common or reused passwords across different services.

Access control policies use mechanisms that define rules and conditions for granting or denying access to resources based on various factors such as user attributes, time of access, location, etc. These policies are put in place to specify anyone who can access as user’s data, when they can do so, and up to which level. These policies need to be implemented accordingly at all

levels of the organization (Satori, 2024).Various access control mechanisms can take many forms such as perimeter-based access controls that use barrier devices in securing a network. Firewalls in the form of packet filters, proxies, and stateful inspection devices are all helpful agents in permitting or denying specific traffic through networks. Access controls also exist on end-user-based systems in the form of a privilege level for access to resources, configuration files, or critical business data (Burton & Dubrawsky, 2003).

Cyber Security Operations Management

Cybersecurity operations and management teams are indispensable for an organization's security defense against cyber threats. The primary cause of many security incidents can be traced back to vulnerabilities within networks that threat actors can exploit to compromise data (Avigdor, 2023) .When security protocols are disregarded, organizations face significant revenue losses because of these breaches. Therefore, the importance of robust security measures must be considered. In today's interconnected digital ecosystem, the scope and complexity of cyber threats are constantly expanding. Attack vectors evolve, tactics become more sophisticated, and new vulnerabilities emerge. Consequently, cybersecurity operations and management teams must remain vigilant and proactive in their approach to cybersecurity. They must stay abreast of the latest threat intelligence, adopt best practices, and leverage advanced technologies to stay ahead of potential threats (Swathi , 2024).An effective cybersecurity department ensures the design, build, operation, and ongoing growth of all facets of the security capability of the organization. The dynamism of a cybersecurity department has many moving parts and must be designed with the ability to adjust and work within the constraints of the organization. It is vital for employee education and training in fostering cybersecurity awareness and the role of communication and collaboration in promoting a collective responsibility towards cybersecurity. To prevent cyberattacks and conform to cyber resilience strategies, an organisation must involve all stakeholders, employees, and customers (Michael, 2023).

Security awareness training is the process of educating people to understand, identify, and avoid cyber threats. The goal is to prevent or mitigate harm to both the organization and its stakeholders and reduce human cyber risk. Cybersecurity awareness training consists of steps taken by utilities to educate all employees about potential cyber threats and their roles in preventing them. While technological solutions significantly protect against cyber threats, employees are often the weakest link in an organization's security infrastructure. The human element in cyber threats is critical because cyber criminals often exploit human vulnerability to access sensitive data or systems (Institute of Data, 2023).Top management of mobile money providers should incentivize good cybersecurity awareness. Employee cybersecurity errors can usually be addressed through additional education and training; sometimes, just the awareness of internal social engineering exercises is enough to motivate better behavior. Where possible, cybersecurity awareness training should be entertaining, humorous, and easy to understand (Harris & Maymi, 2016). The goal is to keep employees engaged long enough that the good cyber habits become a kind of muscle memory (Osterman Research, 2020).

Human cyber resilience represents the overall consciousness of an organization's employees regarding security issues and best practices. To elaborate, it refers to the ability of employees to identify, respond to, and adapt to cyber threats and attacks. Human cyber resilience complements technical and security policy measures to form an organization's overall security posture. It is built individually, with each employee gaining knowledge and skills to recognize threats and make informed, secure decisions (Anilkumar, 2024).A common error that organisations can make, is to think of cyber resilience as a one-time financial spend instead of a financial investment for their future. Rather than an ad hoc or one off spend, it is recommended that organisations consider cyber resilience as a moving target, one that is constantly evolving. Building long-term cyber resilience requires sustained investment and

mobile money providers should consider a separate budget line which demonstrates the organization's commitment to continued protection for the business (Keizer, 2020).
Various guidelines can be followed in defining a cybersecurity budget. Unfortunately, there is no single recommended percentage of turnover that should be spent on cyber resilience. However, based on best practices, some factors heavily affect the budgetary allocation for cybersecurity as; understanding the importance and criticality of risks, size and core business of the organization, as larger organisations with more data and higher risks often need to spend more. Additionally, mobile money providers should focus on spending on high impact areas like cybersecurity awareness training, access controls, data security, incident response plans, and system redundancies (Ursillo & Arnold, 2023).

Incident response is a structured approach to addressing and managing the aftermath of a cybersecurity incident or breach. The primary goal is to handle the occurrence in a way that limits damage, reduces recovery time and costs, and prevents future incidents. Ideally, best practice incident detection, analysis and response plans are implemented under a process of firstly, preparation that identifies assets, then secondly, identification of critical assets and categorize them based on their importance to the organization. Thirdly, an incident response plan (IRP) is developed outlining comprehensive roles, responsibilities, and steps to be taken during an incident or a cyber-attack. Then finally, performing training to the incident response team and simulate regular drills to ensure cyber resilience readiness (Monteiro, 2024). Cyber resilience goes beyond incident response and focuses on an organization's ability to anticipate, prepare for, respond to, and recover from cyber threats. It involves building a holistic and adaptive security posture that can withstand and recover from cyber incidents (Monteiro, 2024).

Empirical Review

A study conducted by PricewaterhouseCoopers (2024) asserted that the significance of digital identity management cannot be understated as effort put in by organizations addressing and investing in proper identity and access management will not only see a reduction in the risk of costly and disruptive cyber-attacks and data loss but will also benefit from better customer and employee experience. Yet digital identity is not something that can be fixed overnight in response to a breach or audit finding. Strong and effective access management requires sustained focus across people, processes, and technologies, from authentication to authorization, user management and provisioning and identity storage and integration.

Another research study conducted by Downs (2024) points out that common risks to IAM in organizations occur when securing identities, whereby most organizations focus on and implement controls around external threat actors. Because of this, overly permissive entitlements often go overlooked leading to more impactful incidents when they do occur. The study advocates prioritizing and enforcing least privilege access with just in time access to data goes a long way in protecting sensitive information from accidental, unauthorized access by insiders. He continues to assert that most IAM vulnerabilities are related to improper configuration, a lack of visibility, poorly defined processes, or a breakdown in processes. Moreover, the study also notes that not keeping up with organizational changes and digital transformations can attribute to one of the biggest challenges researchers continue to see in most environments is excessive permissions accumulated over time, usually by more tenured employees. As roles evolve, employees typically get access to new resources. Over time, this may result in access to a significant portion of the company's information and data.

Another study conducted by Zhu and Ge (2023) argues that despite the long-term solutions that a zero trust mature model propagates to achieve cyber resilience, there are several challenges that arise from the design of zero trust security models. The researchers' note that initially, there is a need to quantitatively define and measure the trustworthiness of the devices so that

metrics can be used for planning and policy design. Secondly, in highly connected networks, constant monitoring and implementing defense with maximum security always can cause a time delay and degrade the performance of the systems. Hence, their study proposes a strategic zero trust needs to be employed for the sake of balancing system performance and security. Lastly, the researchers argue that the mobility and the changing topology of IoT networks can create a dynamic environment and based on the baseline defense policy, the security decisions also need to accommodate the environmental change promptly and craft the policies adaptively with online learning.

A study conducted by Kaur (2021) argues that cyber information sharing between different stakeholders for situational awareness and for organizations to defend themselves is a good cybersecurity best practice and one that always can be improved. The research continues to address the importance of awareness and trainings initiated by organizational top leadership as a crucial step for cybersecurity public awareness and influence the overall organizational cyber resilience journey.

RESEARCH METHODOLOGY

This study focused on a descriptive survey research design and the data was collected from four mobile money providers in Nairobi City County in Kenya. The unit of analysis for this study was mobile money providers in Kenya which includes the four mobile money providers in Nairobi City County Kenya regulated by the Central Bank of Kenya (CBK) namely, Mpesa Africa by Safaricom Ltd, Airtel Money by Airtel Networks Ltd, T-kash by Telkom Kenya and Equitel by Equity's Bank subsidiary, Finserve Africa Ltd. The unit of observation was the employees in various departments that handle the end-to-end mobile money service provisioning, projects and support of mobile money systems and other cross-functional business units. Stratified sampling is defined as a population from which a sample is to be drawn and does not constitute a homogeneous group (Kothari, 2004). He continues to state that stratified sampling technique is generally applied to obtain a representative sample. Under stratified sampling the population is divided into several sub-populations that are individually more homogeneous than the total population. The sub-populations are called strata and items are selected from each stratum to constitute a sample (Kothari, 2004). In the final study, the sample frame was stratified into various groups. There were employees in three categories, senior management, middle level management that included subject matter experts and the low level management operational staff and assistants. The final study focused on an estimated total sample size of 175 respondents across all four mobile money providers. The pilot study dominantly relied on primary research data that was collected using a structured questionnaire. The data was collected, cleaned, coded, and organized before being analyzed. The latest version of SPSS version 29 was used in the analysis and the data was presented majorly using tables. The data was further analyzed through descriptive analysis, relational analysis, and inferential analysis. Multiple regression model was utilized to focus on how the four independent variables would influence the dependent variable. The study used a linear regression model

RESEARCH FINDINGS AND DISCUSSIONS

One hundred and seventy five questionnaires were handed out to management employees from mobile money providers in Nairobi City County in Kenya. From the 175 questionnaires distributed the study received 153 of them having been filled to satisfactory levels. The questionnaires returned added up to 87.7% response rate that was taken to be excellent. This is because according Mugenda and Mugenda (2013), a research achieves a response good enough to proceed with when it attains a 50% response rate, it is sufficient when it is at 60% any response above 70% is considered excellent. Posting an 87.7% response rate the study's response can be employed in the realization of other goals such as reporting.

Descriptive Analysis

In this section , Likert scale questions are presented by the study where research participants were required to give their opinion on several statements concerning the influence of zero trust maturity model in enhancing cyber resilience by mobile money providers in Nairobi City County in Kenya. The research utilized a five-point Likert scale ranked as follows, 1-strongly disagree, 2-disagree, 3-moderate, 4-agree and 5-strongly agree. The standard deviations and means employed in the interpretation of the findings where a mean value of 1-1.4 was strongly disagree, 1.5-2.4 disagree, 2.5-3.4 neutral, 3.5-4.4 agree and 4.5-5 strongly agree. Standard deviation measures the level to which the responses deviate from the mean. A standard deviation greater than two is large and suggests that respondents held varied opinions on the other hand, when research participants had similar opinions a value less than 2 was recorded.

Identity Access Management for Mobile Money Systems

To obtain information about the first independent variable identity access management in mobile money providers, several statements were asked, and the respondents required to provide feedback on a Likert scale of one (1) to five (5), for 1 being strongly disagree, 2 being disagree, 3 being neither agree nor disagree, 4 being agree and 5 being strongly agree to the statements. On the statement "The mobile money system access process is easy for employees in the mobile money department" 5.6% of the respondents disagreed to the statement, 23.5% of the respondents neither agreed nor disagreed to the statement, 33.78% of the respondents agreed to the statement whereas 13.1% of the respondents strongly agreed to the statement, with a mean of 3.78 and standard deviation 0.739. On the second statement "It is simple to perform tasks on mobile money systems for business as usual tasks?" 19.1% of the respondents neither agreed nor disagreed to the statement, 41.0% of the respondents agreed to the statement while 38.9% of the respondents strongly agreed to the statement, with a mean of 4.21 and standard deviation 0.741. On the statement "Employees are required to use multi-factor authentication in accessing all critical systems, 2.8% disagreed with the statement, 38.6% of the respondents neither agreed nor disagreed to the statement, 32.3% of the respondents agreed to the statement whereas 26.3% of the respondents strongly agreed to the statement, with a mean of 3.82 and standard deviation 0.885. Regarding the statement "Biometric authentication would be necessary for accessing critical mobile money systems", 13.1% strongly disagreed to the statement, 10.4% of the respondents disagreed to the statement, 23.9% of the respondents neither agreed nor disagreed to the statement, 35.5% of the respondents agreed to the statement whereas 17.1% of the respondents strongly agreed to the statement, with a mean of 3.33 and standard deviation 1.153.

On the statement "The organization has put in place effective access control policies in mobile money systems." 8.4% strongly disagreed to the statement, 23.9% disagreed to the statement, 23.5% of the respondents neither agreed nor disagreed to the statement, 31.1% of the respondents agreed to the statement whereas 13.1% of the respondents strongly agreed to the statement, with a mean of 3.17 and standard deviation 1.178. On the statement "The organization routinely updates access control mechanisms for mobile money systems." 8.0% strongly disagreed to the statement, 23.9% disagreed to the statement, 26.3% of the respondents neither agreed nor disagreed to the statement, 33.5% of the respondents agreed to the statement whereas 8.4% of the respondents strongly agreed to the statement, with a mean of 3.10 and standard deviation 1.105.

Table 1: Identity Access Management in Mobile Money Systems Frequencies

Identity Access Management in Mobile Money Systems	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Mean	Std. Dev.
The mobile money system access process is easy for employees in the mobile money department	-	5.6	23.5	337.8	13.1	3.78	.739
It is simple to perform tasks on mobile money systems for business-as-usual tasks	-	-	19.1	41.0	38.9	4.21	.741
Employees are required to use multi-factor authentication in accessing all critical systems.	-	2.8	38.6	32.3	26.3	3.82	.885
Biometric authentication would be necessary for accessing critical mobile money systems.	13.1	10.4	23.9	35.5	17.1	3.33	1.153
The organization has put in place effective access control policies in mobile money systems.	8.4	23.9	23.5	31.1	13.1	3.17	1.178
The organization routinely updates access control mechanisms for mobile money systems.	8.0	23.9	26.3	33.5	8.4	3.10	1.105
Average Mean (3.59), S.D (.967)							

Cybersecurity Operations Management in Mobile Money Systems

To obtain information about the first independent variable Cybersecurity Operations Management in Mobile Money Systems, numerous statements were asked, and the respondents required to provide feedback on a Likert scale of one (1) to five (5), for 1 being strongly disagree, 2 being disagree, 3 being neither agree nor disagree, 4 being agree and 5 being strongly agree to the statements. On the statement "The organization has an established cybersecurity department in place and are well-structured" 2.0% strongly disagreed to the statement, 2.8% of the respondents disagreed to the statement, 11.6% of the respondents neither agreed nor disagreed to the statement, 30.7% of the respondents agreed to the statement whereas 53.0% of the respondents strongly agreed to the statement, with a mean of 4.30 and standard deviation 0.922.

On the statement "There is a designated security team responsible for enforcing application and network security policies" 5.6% strongly disagreed to the statement, 7.2% of the respondents disagreed to the statement, 5.6% of the respondents neither agreed nor disagreed to the statement, 53.8% of the respondents agreed to the statement whereas 27.9% of the respondents strongly agreed to the statement, with a mean of 3.91 and standard deviation 1.058. On the statement "My organization has incident response plans in place for security breaches, 5.6% strongly disagreed to the statement, 27.1% of the respondents disagreed to the statement, 19.1% of the respondents neither agreed nor disagreed to the statement, 27.5% of the respondents agreed to the statement whereas 20.7% of the respondents strongly agreed to the statement, with a mean of 3.31 and standard deviation 1.229.

Regarding the statement "Do you believe that regular cybersecurity drills and updated are conducted frequently to ensure the effectiveness of security policies.", 10.4% strongly

disagreed to the statement, 2.8% of the respondents disagreed to the statement, 19.1% of the respondents neither agreed nor disagreed to the statement, 41.8% of the respondents agreed to the statement whereas 25.9% of the respondents strongly agreed to the statement, with a mean of 3.70 and standard deviation 1.188. On the statement "The organization provides cybersecurity adequate budgets" 21.9% strongly disagreed to the statement, 29.1% of the respondents neither agreed nor disagreed to the statement, 39.0% of the respondents agreed to the statement whereas 10.0% of the respondents strongly agreed to the statement, with a mean of 3.15 and standard deviation 1.284.

On the statement "I am aware of the existence of an incident response plan used by the organization" 9.6% of the respondents neither agreed nor disagreed to the statement, 41.0% of the respondents agreed to the statement whereas 49.4% of the respondents strongly agreed to the statement, with a mean of 4.40 and standard deviation 0.658. On the statement "There a dedicated IT security team responsible for monitoring and managing device security across the organization" 2.8% strongly disagreed to the statement, 5.6% of the respondents disagreed to the statement, 47.8% of the respondents neither agreed nor disagreed to the statement, 29.5% of the respondents agreed to the statement whereas 14.3% of the respondents strongly agreed to the statement, with a mean of 3.47 and standard deviation 0.904. Finally, on the statement "There is a well-functioning cybersecurity department in the organization" 7.6% strongly disagreed to the statement, 5.6% disagreed to the statement, 17.9% of the respondents neither agreed nor disagreed to the statement, 52.6% of the respondents agreed to the statement whereas 16.3% of the respondents strongly agreed to the statement, with a mean of 3.65 and standard deviation 1.061.

Table 2: Cybersecurity Operations Management in Mobile Money Systems Frequencies

Cybersecurity Operations Management in Mobile Money Systems	**Strongly Disagree**	**Disagree**	**Neither Agree nor Disagree**	**Agree**	**Strongly Agree**	**Mean**	**Std. Dev.**
Stakeholder's skills are matched with their responsibilities.	2.0	2.8	11.6	30.7	53.0	4.30	0.922
The banks systems are aligned with objectives, strategies and plans of the Bank.	5.6	7.2	5.6	53.8	27.9	3.91	1.058
My organization has incident response plans in place for security breaches.	5.6	27.1	19.1	27.5	20.7	3.31	1.229
Do you believe that regular cybersecurity drills and updated are conducted frequently to ensure the effectiveness of security policies.	10.4	2.8	19.1	41.8	25.9	3.70	1.188
The organization provides cybersecurity adequate budgets	21.9	-	29.1	39.0	10.0	3.15	1.284
I am aware of the existence of an incident response plan used by the organization.	-	-	9.6	41.0	49.4	4.40	0.658
The organization regularly reviews and updates staff about cybersecurity information	2.8	5.6	47.8	29.5	14.3	3.47	0.904
There is a well-functioning cybersecurity department in the organization.	7.6	5.6	17.9	52.6	16.3	3.65	1.061
Average Mean (3.74), S.D (1.038)							

Correlation Analysis for Identity Access Management in Mobile Money Systems

Table 3 below shows that there were strong positive significant relationships between Identity Access Management in Mobile Money Systems and all other independent variables and the moderating variables. The correlation coefficients were 0.598, 0.780, 0.617, and 0.540, all with p-values less than 0.001.

Table 3: Correlation matrix for Identity Access Management in Mobile Money Systems Variable

		Y	X_1	X_2	X_3	X_4
X_1	Pearson Correlation	.653**	1	.598**	.780**	.617**
	Sig. (2-tailed)	0		0	0	0
	N	153	153	153	153	153

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

Correlation Analysis for Cybersecurity Operations Management in Mobile Money Systems

Table 4 below shows that there were strong positive significant relationships between Cybersecurity Operations Management in Mobile Money Systems and Identity Access Management in Mobile Money Systems. The correlation coefficients were 0.598, 0.804, 0.872, and 0.817, all with p-values less than 0.001.

Table 4: Correlation matrix for Cybersecurity Operations Management in Mobile Money Systems Variable

Correlations		Y	X_1	X_2	X_3	X_4
X_2	Pearson Correlation	.763**	.598**	1	.804**	.872**
	Sig. (2-tailed)	0	0		0	0
	N	153	153	153	153	153

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

Regression Coefficients of the Study Variables

This regression equation model was used to fit the regression coefficient.

$$\mathbf{Y = 1.347 + 0.347\ X_1 + 0.338\ X_2}$$

Observing the equations, it can be noted that when all the other variables remain at constant zero, a constant value of 1.347 was held by the cyber resilience. The results depict identity access management in mobile money systems significantly impacting cyber resilience (β=0.347, p=0.001). These results insinuate that identity access management in mobile money systems is significantly influences cyber resilience in a positive way. Meaning, a unit rise in identity access management in mobile money systems leads to a rise in cyber resilience, by 0.347 units. Mellado et al. (2019) emphasizes that IAM is crucial for securing mobile financial systems by preventing unauthorized access, thus enhancing overall cyber resilience. Additionally, He and Xu (2020) found that improved IAM frameworks in digital financial services lead to better system defenses against cyberattacks, contributing to resilience. Furthermore, research by Shen et al. (2021) highlights that strengthening IAM positively correlates with a system's ability to withstand and recover from security breaches, aligning with the study's findings.

Cybersecurity operations management in mobile money systems has an influence on cyber resilience (β=0.338, p=0.018). The studies also revealed that decision-making procedures on investment had a desirable impact on cyber resilience. These findings imply that investing

decision-making procedures exhibit a favorable impact on cyber resilience. As a result, a unit increase in cybersecurity operations management in mobile money systems processes leads to a 0.338 unit rise in the cyber resilience. Research by He and Xu (2020) found that proactive cybersecurity management, including regular monitoring, incident response strategies, and system updates, directly enhances a system's resilience against cyber threats. In mobile money systems, which are highly susceptible to digital fraud and cyberattacks, strong cybersecurity operations can mitigate these risks and ensure service continuity, supporting the study's results.

Table 4.34: Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.347	0.258		5.221	.000
	Identity access management	0.347	0.103	0.439	3.369	.001
	Cybersecurity Operations Management	0.338	0.138	0.402	2.449	.018

a. Dependent Variable: Cyber Resilience

Conclusion

Identity access management emerged as a key factor, demonstrating that secure user authentication and access control are vital for protecting against unauthorized access and ensuring system integrity. Effective IAM practices not only prevent breaches but also reinforce user trust in mobile money platforms. Similarly, the impact of cybersecurity operations management emphasizes the need for proactive threat detection and response strategies to maintain system stability and resilience in the face of evolving cyber threats.

Recommendations

Based on the study’s findings, it is recommended that mobile money providers prioritize enhancing their Identity Access Management (IAM) systems. Implementing robust IAM practices, including multi-factor authentication, regular access reviews, and stringent user verification processes, is essential for safeguarding sensitive financial data and preventing unauthorized access. By investing in advanced IAM technologies and continuously updating their security protocols, providers can significantly improve their cyber resilience and protect against potential security breaches.

Lastly, it is vital for mobile money providers to invest in cybersecurity operations management. Establishing proactive cybersecurity operations, such as continuous threat monitoring and incident response strategies, can help detect and mitigate cyber threats more effectively. Simultaneously, robust data security practices, including encryption and secure data handling, are critical for by adopting a holistic approach that integrates these security measures, mobile money providers can build a resilient framework capable of defending against evolving cyber threats and ensuring the reliability of their financial services.

Suggestions for Further Research

Future research should explore the impact of emerging technologies and trends on the security and resilience of mobile money systems. As digital financial services continue to evolve, new technologies such as blockchain, artificial intelligence, and machine learning are becoming increasingly relevant. Investigating how these technologies can be integrated into existing cybersecurity frameworks to enhance resilience and address new types of threats could provide

valuable insights. Additionally, examining the effectiveness of advanced security technologies in various contexts and their practical implementation challenges would contribute to a deeper understanding of their potential benefits.

REFERENCES

Aiello Samuel (2022). *Zero Trust: A Governance Perspective*. Retrieved from https://ssrn.com/abstract=4146521 or http://dx.doi.org/10.2139/ssrn.4146521

Ambore and Richardson, et al. (2017). *A Resilient Cybersecurity Framework for Mobile Financial Services (MFS). Journal of Cyber Security Technology*.DOI.org (Crossref). Retrieved from https://doi.org/10.1080/23742917.2017.1386483.

Aubra Anthony, Nanjira Sambuli, and Lakshmee Sharma (2024).*Security and Trust in Africa's Digital Financial Inclusion Landscape*. Retrieved from https://carnegieendowment.org/research/2024/03/security-and-trust-in-africas-digital-financial-inclusion-landscape?lang=en&center=europe

Benoît Dupont (2019). *The Cyber-Resilience of Financial Institutions: Significance and Applicability. Journal of Cybersecurity*. DOI.org (Crossref). Retrieved from

Bryman, A. (2016). *Social Research Methods* (5th ed.). London: Oxford University Press.

CISA (2024) *Zero Trust Maturity Model: Cybersecurity and Infrastructure Security Agency CISA.* Retrieved from https://www.cisa.gov/zero trust-maturity-model

Cisco (2023). *Security Outcomes for Zero Trust: Adoption, Access, and Automation Trends*. Retrieved from https://www.cisco.com/c/dam/en/us/solutions/collateral/security/zero trust/zero trust-outcomes.pdf

Craig, T., & Ludloff, M.E. (2011). *Privacy and Big Data: The Players, Regulators, and Stakeholders.* Published by O'Reilly Media, Inc.,1005

De Groot, J. (May 21,2024). *What is data encryption? (definition, best practices & more). Digital Guardian.* Retrieved from https://www.digitalguardian.com/blog/what-data-encryption

Dell (May 22, 2024) *Cyber Resilience -Cyber Protection. (n.d.).* Retrieved from https://www.dell.com/en-us/dt/learn/data-protection/cyber-resilience.htm

DesignRush (2024).Retrieved from https://www.designrush.com/agency/cybersecurity/trends/user-authentication

Downs, M. (2024, February 12). *Cyber resilience for identity and access management. Evolving Solutions.* Retrieved from https://evolvingsol.com/identity-and-access-management-cyber-resilience/

Flanigan, J. (2018). *Zero Trust Network Model*. Tufts University: Medford, MA, USA. Retrieved from https://www.cs.tufts.edu/comp/116/archive/fall2018/jflanigan.pdf

Government of Canada (2022). *Canadian Center for Cyber Security: A zero trust approach to security architecture* (ITSM.10.008). [Publication]. Retrieved from

Gurdip Kaur, Ziba Habibi Lashkari, Arash Habibi Lashkari (2021) *Understanding Cybersecurity Management in FinTech; Challenges, Strategies, and Trends*. Springer Charm.
https://doi.org/10.1093/cybsec/tyz013

Lloyd, J. (2023). *BeyondCorp. In: Infrastructure Leader's Guide to Google Cloud*. Apress, Berkeley. CA. Retrieved from https://doi.org/10.1007/978-1-4842-8820-7_29

Maricus Otieno Mayunga (2019).*Developing and Assessing A Cyber-Resilience Framework For Kenyan Banks.*

MarshMcLennan (2024).*The State of Cyber Resilience – Asia and Global insights*. Retrieved from https://www.marsh.com/my/services/cyber-risk/insights/the-state-of-cyber-resilience.html#sizetracker

Martin Walter (2024)*Data insecurity: Building resilience in the face of cyber threats. (n.d.).* Retrieved from https://www.rubrik.com/blog/technology/24/2/data-insecurity-building-resilience-in-the-face-of-cyber-threats

Maya, G. (2021, August 13). *Backup and recovery policy - Protect Your Data with a Documented Plan. ITSM Docs - ITSM Documents & Templates*. Retrieved from https://www.itsm-docs.com/blogs/security-management/backup-and-recovery-policy

Mercy W. Buku & Rafe Mazer (2017). *Brief Fraud in Mobile Financial Services: Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System.* CGAP Publication.

Mugenda, O. and Mugenda (2008).*Social Sciences Research*: Theory and Principles. ART

Ömer Aslan, Semih S.Aktuğ, et.al (2023). *A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions.* Retrieved from https://www.mdpi.com/2079-9292/12/6/1333.

Patrick Van Eecke,Yasmin Roland (2024).*Building Cyber Resilience in the Financial Services Sector: New Rules in Europe*. Retrieved from https://cdp.cooley.com/building-cyber-resilience-in-the-financial-services-sector-new-rules-in-europe/

Phil Robinson (2023).Retrieved from https://www.architectureandgovernance.com/elevating-ea/is-zero-trust-achievable/

Positive Technologies (July 28,2023). *Cybersecurity threatscape of African countries 2022–2023*.Retrieved from https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/

Presence Secure (2024).Retrieved from https://www.presencesecure.com/zero-trust-to-cyber-resilience/

PricewaterhouseCoopers (2024). *Digital identity at the heart of cyber resilience and experience. PwC.* Retrieved from https://www.pwc.com.au/cyber-security-digital-trust/digital-identity.html

Rogers, E. M. (2003). *Diffusion of Cybersecurity Operations Management s, 5th Edition (5th ed.).* Free Press.

Rose, S., Borchert, O., et.al (2020). *Zero Trust Architecture, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD.* Retrieved from https://www.nist.gov/publications/zero trust-architecture.

Sarkar, Choudhary, et al. (2022). *Security of Zero Trust Networks in Cloud Computing: A Comparative Review.* Publication. Retrieved from https://doi.org/10.3390/su141811213

Shepherd, Cody (2022).*Zero Trust Architecture: Framework and Case Study; Cyber Operations and Resilience Program Graduate Projects*. Retrieved from https://scholarworks.boisestate.edu/cyber_gradproj/1

Shorna Broussard Allred & Amy Ross-Davis (2011).*The Drop-off and Pick-up Method: An Approach to Reduce Nonresponse Bias in Natural Resource Surveys*.Publication.DOI:10.1007/s11842-010-9150-y

Yale School of Management Case Study (2024).Retrieved from https://workshop1.cases.som.yale.edu/mpeso/background/mobile-money

ZenGRC (2024).*Threat, Vulnerability, and Risk: What's the Difference?* Retrieved from https://reciprocity.com/blog/threat-vulnerability-and-risk-whats-the-difference/