CONTEXT AWARENESS VULNERABILITIES DETECTION MODEL IN BYOD ENVIRONMENT USING A LINEAR REGRESSION TECHNIQUE.

BY

JEREMIAH N WANJIRU

MASTER OF SCIENCE INFORMATION SYSTEMS MANAGEMENT

KCA UNIVERSITY

2025

CONTEXT AWARENESS VULNERABILITIES DETECTION MODEL IN BYOD ENVIRONMENT USING A LINEAR REGRESSION TECHNIQUE

By

JEREMIAH N WANJIRU.

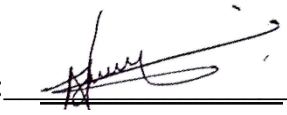
A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE DEGREE IN INFORMATION SYSTEMS MANAGEMENT IN THE SCHOOL OF TECHNOLOGY AT KCA UNIVERSITY.

JANUARY 2025

DECLARATION

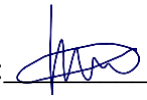
I declare that this project is my original work and has not been previously published or submitted elsewhere for award of a degree. I also declare that this project contains no material written or published by other people except where due reference is made, and author duly acknowledged.

Student Name : Jeremiah Njoroge Wanjiru Reg No: 11/00108

Sign:  Date: 17/01/2025

I do hereby confirm that I have examined the master's dissertation of
Jeremiah Njoroge Wanjiru

And have certified that all revisions that the dissertation panel and examiners recommended have been adequately addressed.

Sign:  Date: 18/01/2025

Dr. Lucy Waruguru Mburu
Dissertation Supervisor

CONTEXT AWARENESS VULNERABILITIES DETECTION MODEL IN BYOD ENVIRONMENT USING A LINEAR REGRESSION TECHNIQUE.

ABSTRACT

The purpose of this study was to examine context-awareness vulnerabilities in Bring Your Own Device (BYOD) environments within large SACCOs in Kenya. Adoption of BYOD practices, enable employees of an organization to use personal devices for work. In the recent past there has been incidents of financial vulnerabilities, including losses attributed to both internal collusion and external cyber-attacks, which showed the urgent need for solutions focused on vulnerability detection mechanisms. The analysis of past literature revealed gaps in existing models, which inadequately address SACCO-specific risks such as the role-based access and dynamic access patterns, often relying on a narrow set of data points or reliance of static approaches. The study employed a descriptive survey design, using structured questionnaires to collect data from 86 employees of Mwalimu SACCO's head office in Nairobi. As the largest SACCO in Kenya, Mwalimu SACCO provided a suitable context to analyse BYOD-related vulnerabilities in a high-risk, resource-constrained environment. Descriptive techniques and multivariate regression analysis were employed to determine the influence of the identified factors on the vulnerability index. The study findings showed that access time, location, and role risk factors significantly wielded and affect vulnerability in BYOD environments. Access time emerged as the most critical determinant, with increased risks observed during non-standard work hours. Location vulnerabilities were heightened in remote settings due to limited security measures, while role risk factors indicated that employees with elevated access privileges, particularly in ICT and finance roles, posed greater risks. The study formulated a multivariate regression model which demonstrated high predictive accuracy, with an R^2 value of 0.89 and a mean absolute error of 0.12. These results validated its reliability in identifying and predicting context-awareness vulnerabilities in SACCO BYOD environments. The study concludes that, there is increased use of personal devices by SACCO staff to undertake both personal and official engagements. Further, the study concludes that, there is lack of comprehensive BYOD policies that conforms to prevailing vulnerabilities. Through adoption of robust access controls, organization centered BYOD policies, and role-specific security measures, SACCOs can upscale their defences. These measures would enable SACCOs to mitigate vulnerabilities, reduce insider fraud and external threats, and strengthen their cyber-security posture. This research fills a critical gap in understanding and managing context-aware vulnerabilities in BYOD environments, offering a practical framework for enhancing the security of SACCO operations in Kenya.

Keywords: BYOD, SACCOs, context-aware, vulnerabilities

ACKNOWLEDGMENT

At the onset, I express my sincere gratitude to the Almighty God for granting me good health, strength, and the unwavering desire to see this study through to completion. His blessings and guidance have been my anchor throughout this journey.

I am deeply grateful to my supervisor, Dr. Lucy Waruguru, of KCA University's School of Technology, for her invaluable guidance, constructive feedback, and encouragement. Her expertise and support played a pivotal role in shaping this study and ensuring its success. Her dedication to excellence and her insightful advice inspired me to strive for the best.

I extend my sincere appreciation to KCA University and the School of Technology for providing a conducive learning environment and the resources necessary for this study. The knowledge and skills imparted to me have been instrumental in undertaking and completing this research.

To my classmates, I express my heartfelt thanks for their camaraderie, insightful discussions, and support during our academic journey. The collaborative spirit and shared experiences enriched my understanding and made this process more rewarding.

DEDICATION

This work is lovingly dedicated to my family, whose unwavering support, encouragement, and unconditional love have been my greatest source of strength throughout my academic journey. Thank you for your endless sacrifices and belief in my dreams, and your constant motivation and care. Your faith in me has been my inspiration, and your support has made this achievement possible. This milestone is as much yours as it is mine, thank you for always being there for me.

LIST OF ACCRONYMS AND ABBREVIATIONS

BYOD	Bring Your Own Device
ISM	Information Security Management
IT	Information Technology
MDM	Mobile Device Management
RAdAC	Risk-Adaptable Access Control Model
RBAC	Role-Based Access Control
RCT	Rational Choice Theory
SACCOs	Savings and Credit Cooperative Societies
SASRA	SACCO Societies Regulatory Authority
SME	Small and Medium Enterprises
TAM	Technology Acceptance Model
TRA	Theory of Reasoned Action
CAV	Context Awareness Vulnerability

DEFINITION OF KEY TERMS

Context Awareness Vulnerabilities	These refer to security risks arising from the inability to adapt security protocols based on environmental factors such as user behaviour, device characteristics, and location in BYOD settings.
BYOD (Bring Your Own Device)	A policy allowing employees to use personal devices, such as smartphones or laptops, for work-related tasks, increasing flexibility but introducing security risks.
BYOD Environment	A workplace setup where employees use their personal devices to access corporate networks and data, requiring adaptive security measures to manage vulnerabilities.
Access Time	The specific time an employee or device accesses a system, which can be a critical factor in identifying potential security risks or abnormal usage patterns.
Device Usage	Refers to how and for what purposes personal devices are used within a BYOD environment, impacting the potential exposure to security vulnerabilities.
Location	The geographic or network-based location from which a device accesses the system, a factor in determining potential security risks due to varying network security levels.
Role Risk Factor	The security risk associated with an employee's role, based on the sensitivity of data they access and their level of system permissions in the BYOD environment.
Vulnerability Score	A quantifiable measure of the potential security risks associated with context awareness factors like access time, device usage, location, and role in a BYOD environment.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 Background to the study

In today's rapidly evolving digital landscape, the integration of personal devices into professional environments, commonly referred to as Bring Your Own Device (BYOD), has become increasingly prevalent (Aguboshim, Udobi & Otuu, 2023; Klein & Zwilling, 2024). This trend reflects the growing desire for flexibility and efficiency, allowing employees to use their own smartphones, tablets, and laptops to access corporate resources and perform work tasks. The BYOD approach facilitates improved productivity, operational agility, and job satisfaction, as employees can work from various locations and have access to familiar technology (Bernhardt, Kresge & Suleiman, 2023). However, it also introduces significant cyber-security challenges that must be carefully managed.

As organizations increasingly embrace BYOD technology for its numerous benefits, such as enhanced employee productivity, flexibility, and reduced hardware costs, they also face significant challenges and potential disadvantages (Jamal et al., 2020). One of the primary concerns revolves not just around the devices themselves or the data stored within the organization, but more critically around controlling and securing access to organizational information from a diverse array of personal devices (Bernhardt et al., 2023). The decentralized nature of BYOD complicates this control, as it limits the organization's ability to monitor and manage the security of these devices effectively (Ferdousi, 2022).

The main risks in BYOD environments stem from the difficulty in ensuring that only authorized users and secure devices can access sensitive organizational data (Jimshith, 2024; Wani et al., 2022). Personal devices often lack the stringent security protocols and updates that are standard in corporate-owned devices, making them vulnerable to malware, phishing attacks, and unauthorized access. This vulnerability is further increased by the lack of visibility

that organizations have over these devices, particularly when they connect to the corporate network from external locations or through unsecured public Wi-Fi (Jamal, et al.2020).

The increased exposure of enterprise networks to potential threats, such as malware and data breaches, underscores the urgent need for more robust strategies to identify and mitigate these risks (Rah, 2023; Veljkovic & Budree, 2019). As BYOD adoption continues to grow across various industries, particularly in corporate organizations, there is a pressing need to develop and implement advanced methods for detecting vulnerabilities and managing risks (Ozer et al., 2024). These strategies must focus on enhancing control over access points and improving visibility into device security, ensuring that the benefits of BYOD do not come at the cost of organizational security.

For financial institutions, which handle highly sensitive and critical data such as personal identification information, transaction details, and financial records, the implications of BYOD are particularly concerning (Chigada, J., & Daniels, 2021; Ofusori, 2019). These institutions are prime targets for cyber-attacks due to the valuable nature of their data and the potential financial impact of breaches (Mphahlele, 2024). The integration of personal devices into their networks exacerbates the risk of unauthorized access, data leaks, and malware infections, as these devices are often less secure than corporate-owned and managed hardware.

The proliferation of BYOD practices in the workplace has brought about a paradigm shift in how organizations manage security (Jimshith, 2024). Traditionally, companies maintained strict control over the devices and networks used by employees, ensuring that all access points were secure and monitored. However, BYOD has decentralized this control, as employees now use a diverse array of personal devices to access corporate networks and data (Shukry et al. 2023). This decentralization complicates the enforcement of security policies and the monitoring of potential threats, creating a fertile ground for cybersecurity vulnerabilities.

Among these financial entities, large Savings and Credit Cooperative Organizations (SACCOs) face distinct challenges. Unlike major banks with extensive cyber-security resources and infrastructure, SACCOs frequently operate with more limited budgets and less advanced security measures (Mbugua, 2020). This makes them particularly vulnerable in BYOD environments, where inconsistent device security, inadequate management of personal devices, and limited IT oversight can lead to significant security gaps (Wanjala & Riitho, 2020). As SACCOs increasingly adopt BYOD practices to enhance operational flexibility and member services, addressing these cyber-security challenges becomes crucial to safeguarding their sensitive data and maintaining trust with their members.

The importance of cyber-security in BYOD environments cannot be overstated, particularly for institutions that deal with sensitive financial information. Cyber threats such as phishing, malware, unauthorized access, and data breaches are amplified in BYOD settings due to the inherent lack of uniformity in device security. Each personal device comes with its own set of vulnerabilities, often determined by factors such as outdated software, weak passwords, and unpatched security flaws. Moreover, the use of personal devices for both work and private purposes increases the likelihood of inadvertent exposure to malicious content or networks.

1.1.1 BYOD in financial institutions and large SACCOs

In financial institutions, the level of risk consideration is particularly high (Wangu, 2021). These organizations are entrusted with safeguarding vast amounts of sensitive data, including personal identification information, financial records, and transaction histories. A breach in security could not only result in financial loss but also lead to a loss of customer trust, legal repercussions, and damage to the institution's reputation (Koskei, 2019). Consequently, the adoption of BYOD practices in financial institutions necessitates a robust cyber-security strategy that can effectively mitigate the risks associated with the use of personal devices.

Despite the known risks, many financial institutions have embraced BYOD due to its potential benefits. These benefits include cost savings on hardware, increased employee satisfaction, and the ability to maintain business continuity by allowing employees to work remotely or during travel. However, these advantages must be weighed against the security challenges that BYOD introduces (Mwendwa, 2021). The complex nature of financial operations, coupled with the sensitivity of the data involved, makes financial institutions prime targets for cyber-attacks. In this context, the need for enhanced cyber-security measures in BYOD environments is both urgent and critical (Koskei, 2019).

Large SACCOs, in particular, face distinct cyber-security challenges within the BYOD framework. SACCOs are member-owned financial cooperatives that provide a wide range of financial services, including savings accounts, loans, and insurance (Wanjala & Riitho, 2020). While they share similarities with banks, SACCOs often operate with more limited resources, particularly in terms of cyber-security infrastructure and expertise (Mwendwa, 2021). This makes them more vulnerable to cyber threats, especially as they increasingly adopt BYOD practices to improve operational efficiency and member service.

The decentralized and often diverse nature of SACCO operations increases the challenges associated with BYOD (Koskei, 2019). Unlike larger banks, SACCOs may not have the same level of centralized IT management or security oversight (Wangu, 2021). This can lead to inconsistencies in how BYOD policies are implemented and enforced across different branches or departments. Furthermore, employees in SACCOs may use a wider variety of devices, each with varying levels of security, making it difficult to maintain a uniform security standard. One of the primary concerns for SACCOs in a BYOD environment is the risk of unauthorized access to sensitive financial data. Personal devices are more likely to be lost, stolen, or compromised, which can lead to unauthorized individuals gaining access to the institution’s network and data. Additionally, the use of unsecured public Wi-Fi networks, a

common practice among employees using personal devices, further increases the risk of data interception and cyber-attacks.

Another significant challenge is the management of data privacy and compliance with regulatory requirements (SASRA, 2022). SACCOs, like all financial institutions, are subject to stringent regulations regarding the protection of customer data. Ensuring compliance with these regulations in a BYOD environment can be challenging, particularly when employees use devices that are not fully under the control of the institution's IT department. The risk of data leakage is heightened when employees store sensitive information on personal devices, which may not have adequate encryption or data protection measures in place.

1.1.2 Understanding risks for BYOD in SACCOs and importance of vulnerability detection

Given the unique challenges that large SACCOs face in BYOD environments, there is a critical need for a predictive model that can help identify and mitigate context awareness vulnerabilities. Context awareness in cyber-security refers to the ability to understand and respond to the contextual factors that influence the security of an environment. In the case of BYOD, these factors may include the time and location of device usage, the nature of the employee's role within the organization, and the specific activities being conducted on the device.

A predictive model based on linear regression can provide valuable insights into the likelihood of context awareness vulnerabilities within SACCOs. By analysing data related to employee behaviour and device usage, the model can identify patterns and correlations that indicate a heightened risk of security breaches. This approach allows SACCOs to proactively address potential threats before they materialize, enhancing the overall security of their BYOD environments.

The conceptualization of the model could integrate variables that deduce number of hours an employee accesses the network outside of regular working hours, the frequency of

location changes, and the risk level associated with the employee's role. By assigning a vulnerability score based on these factors, SACCOs can prioritize their security efforts, focusing on the employees or devices that pose the greatest risk.

1.1.3 Linear regression model in vulnerability detection within BYOD environment

A linear regression model is a statistical technique used to analyze relationships between one or more independent variables and a dependent variable (Hoffmann, 2021). The model is underpinned in assumption for linear relationship, which means changes in independent variables lead to proportional changes in the dependent variable (Ottaviani & De Marco, 2022). Linear regression is valued for its simplicity, interpretability, and predictive power, making it a go-to model for analyzing patterns and identifying risk factors (Korystin, Nataliia & Mitina, 2022). Its ability to quantify relationships between variables makes it a powerful tool for decision-making, especially in security analysis, finance, and risk management. The concept of Bring Your Own Device (BYOD) has emerged as a unique approach in today's working environment, bringing about flexibility, through giving employees freedom to access organizational systems via personal devices (Eke, Norman & Mulenga,2023).

This convenience has come with significant security challenges, particularly in relation to context awareness vulnerabilities, which encompass risks associated with factors like access time, geographic location, and user roles (Staffans, 2024). In order to address these vulnerabilities, an effective detection and mitigation strategies are required. Linear regression model, offer unique dimension that enables understanding and predicting vulnerabilities within BYOD environments. Its application, involves establishing relationships between independent variables (such as access time, device usage, location, role) and a dependent variable (vulnerability index). Linear regression model provides clear, interpretable insights into how specific factors contribute to security risks. This transparency enables organizations, such as

Savings and Credit Cooperative Organizations (SACCOs), to implement targeted, data-driven security policies in an effective and reliable manner.

Whereas existing evidence shows that advanced machine learning techniques have been explored for BYOD security, they often introduce complexity and require substantial computational resources. The prominence of models such as Support Vector Machines (SVM), Decision Trees (DT), and Random Forests (RF) offer broad utility in addressing BYOD security threats. However, these models present closed source, thus lacking the interpretability crucial for practical decision-making in resource limited environments such as that of SACCOs. Further, the application of machine learning in context-aware security has been primarily focused on environments such as smart homes and internet-of-things (IoT) systems. In application for context-aware IoT-driven security scheme such as in smart homes concept, these models rely on adaptive security measures based on contextual information. Methods like deep learning have been proposed for context-aware security in BYOD settings, but their complexity and resource requirements can hinder practical implementation. While insightful, these approaches may not directly translate to the unique challenges presented by BYOD policies in SACCOs. In contrast, linear regression model, brings about simplicity and ease of implementation, making them particularly suitable for SACCOs aiming to enhance their BYOD security frameworks without incurring significant computational overhead. By leveraging linear regression, SACCOs can effectively identify and mitigate context-aware vulnerabilities, thereby safeguarding sensitive information and maintaining operational integrity in an increasingly mobile-centric work environment.

1.2 Statement of the Problem

The financial services sector in Kenya has experienced significant growth over the past two decades, driven by innovations such as mobile money, which has been widely adopted (Lepoutre & Oguntoye, 2018). Financial institutions, including commercial banks, micro-

finance institutions (MFIs), and Savings and Credit Cooperative Organizations (SACCOs), have expanded their customer bases and transaction volumes. SACCOs, in particular, have become essential for many Kenyans from various socio-economic backgrounds. However, this growth has also exposed SACCOs to increasing instances of fraud and security threats. Between 2022 and 2023, SACCOs reported significant financial losses due to fraud. An audit of Metropolitan SACCO in 2022 revealed a loss of approximately Ksh. 7.2 billion due to fraudulent staff activities (Ciuri, 2023). In 2023, the SACCO Societies Regulatory Authority (SASRA) reported that SACCOs lost an estimated Ksh. 118.1 million to insider fraud (SASRA, 2023). Furthermore, 12 employees of Njiwa SACCO were charged with stealing Ksh. 160 million from members' savings in 2023. These incidents highlight the growing problem of insider fraud, emphasizing the need to investigate staff activities and develop effective strategies to safeguard SACCOs' financial security.

One critical area of concern is the use of personal devices in work environments, commonly referred to as Bring Your Own Device (BYOD). The integration of BYOD in SACCOs presents several challenges, especially in protecting sensitive data from unauthorized access, data breaches, and other cyber-security threats. Given the complex nature of financial institutions and the sensitive information they manage, SACCOs are particularly vulnerable to these risks. Unlike larger financial institutions with robust security infrastructure, SACCOs typically operate with limited resources and decentralized operations, making them attractive targets for cyber-attacks.

Numerous past studies have proposed models for tackling vulnerabilities in BYOD contexts. Balega et al. (2024) explored anomaly detection in IoT and BYOD using XGBoost, SVM, and DCNN. XGBoost achieved 99.98% accuracy and was computationally efficient, but the study relied on specific datasets, limiting generalizability. Chizoba and Kyari (2020) focused on Advanced Persistent Threats (APTs), employing an ensemble of SVM, Random

Forest, and Decision Tree models. Their approach achieved 90.47% accuracy but was constrained by simulated datasets, limiting applicability to real-world BYOD scenarios. Munuo (2024) applied Zero Trust Architecture (ZTA) in the financial sector with Logistic Regression, Random Forest, XGBoost, and Time Series Analysis, highlighting ZTA's security benefits. However, the experimental architecture lacked diversity, affecting precision and recall. Ussatova et al. (2023) developed a scanner for SQL injection detection using models like Naïve Bayes, Logistic Regression, and XGBoost, yet overlooked broader BYOD vulnerabilities. Shah and Shankarappa (2018) proposed a risk management framework for BYOD using SVM, MLP, BN, and RF, relying heavily on MDM logs. These models inadequately address SACCO-specific vulnerabilities like role-based access risks. The past models have not shown contextual vulnerabilities specific to SACCO environments, such as role-based access risks, insider threats, and dynamic access patterns in BYOD settings. In addition they also rely on narrow datasets and static architectures, limiting adaptability. This shows the existing gaps in regard to emerging financial institutions like SACCOs.

The problem of context awareness vulnerabilities in SACCOs' BYOD environments emerges due to uncontrolled access risks linked to access time, location level, and role risk factors. The current study sought to employ a linear regression approach which integrates variables notably access time, location level, and role risk factors, providing a tailored and comprehensive vulnerability detection framework for SACCOs. Without a clear understanding of how these variables influence security risks, SACCOs struggle to implement effective mitigation strategies. Linear regression provides a structured, quantitative approach to model these relationships, offering predictive insights into vulnerability trends. By analyzing historical access patterns, the model helps identify high-risk scenarios, allowing SACCOs to adjust security measures proactively. Unlike complex machine learning models, linear regression ensures interpretability, enabling decision-makers to implement targeted security

controls based on empirical evidence. This solution enhances context-aware security measures, reducing unauthorized access risks in resource-constrained SACCO environments. This targeted approach will fill a critical gap in existing research and offer valuable insights into improving the security set-up of SACCOs in Kenya.

1.3 Objectives of the Study

1.3.1 Main Objective

The main objective in this study is to develop a context awareness vulnerabilities detection model for BYOD environments within large SACCOs in Kenya using a Linear regression technique.

1.3.2 Specific Objectives

The study was guided by the following objectives;

i. Investigate Contextual factors that influence vulnerabilities in BYOD environment.
ii. Design and develop a regression model for BYOD using the identified factors.
iii. Test and validate the model.

1.4 Research Questions

The study sought to answer the following questions;

i. What factors cause context awareness vulnerabilities in BYOD environment?
ii. Will the model successfully aid in context awareness vulnerability detection in BYOD environment?
iii. To what extent will the model be used to detect context awareness vulnerabilities in the BYOD environment?

1.5 Significance

The findings of this study offers substantial benefits to various stakeholders, including the management of SACCOs, SACCO members, policymakers in government, and the academic community.

For SACCO management, they gain an additional tool to monitor employee activities as they use personal devices for work. By understanding and identifying context awareness vulnerabilities, management will be better equipped to detect potential risks and implement appropriate mitigation strategies, thereby safeguarding organizational data and operations. This proactive approach will enhance the overall security framework within SACCOs, ensuring that sensitive information is protected from unauthorized access or breaches.

SACCO members will also benefit significantly from the findings of this study. As security measures are strengthened, members can have greater confidence in the safety of their savings and investments. Furthermore, the increased efficiency and convenience of SACCO services, enabled by employees' use of personal devices, will enhance the overall customer experience, making it easier for members to access and manage their accounts.

Policymakers in government will gain valuable insights from this research, particularly regarding the formulation of new regulations, reforms, and policies that address the evolving security challenges posed by BYOD strategies in SACCOs. The study will provide evidence-based recommendations that can inform the development of robust legal frameworks aimed at protecting financial institutions and their clients in the digital age.

Finally, researchers and academicians will find this study to be a valuable resource for understanding BYOD and context vulnerabilities within the financial services sector, specifically in SACCOs. The research will serve as a reference point for future studies, offering insights into areas that require further exploration and contributing to the broader body of knowledge in this field.

1.6 Motivation of the Study

BYOD is increasingly recognized as a strategic approach that will continue to gain traction within corporate environments, offering employees the convenience of using their personal mobile devices to access organizational information and data. As this trend grows, particularly

within SACCOs, the exposure to context awareness vulnerabilities also escalates. SACCOs, which handle sensitive financial data, are particularly at risk due to the diverse and often unsecured nature of personal devices. The integration of these devices into corporate networks presents unique challenges, especially in maintaining the security and integrity of critical operations and member information. Given the expanding role of BYOD in SACCOs, there is an urgent need to address the associated cyber-security risks. This study is motivated by the necessity to develop a robust model that can help SACCOs detect and manage risk levels related to context awareness vulnerabilities. By focusing on these vulnerabilities, the study aims to provide SACCOs with the tools needed to safeguard their data and ensure secure access across their BYOD environments, thereby enhancing overall organizational resilience.

1.7 Scope of the Study

This study aims to examine context awareness vulnerabilities within BYOD environments specifically in large SACCOs. The research will focus on Mwalimu National SACCO, which is the largest SACCO in Kenya in both membership numbers and savings (Maina, 2023). The SACCO has extensive operations, with multiple branches and employing over 1,200 staff members. Given the scale and complexity of its operations, this SACCOs present an ideal context for studying the cyber-security challenges associated with BYOD practices. The scope of the study will be further narrowed to the headquarters of the SACCO, where critical staff and data operations are concentrated. By focusing on the central hub, the research will gain insight into the most significant vulnerabilities in BYOD environments, particularly those that could affect sensitive financial data and critical decision-making processes. The study will also consider how these vulnerabilities might impact the broader network of branches connected to the headquarters, providing a comprehensive analysis of the risks involved.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This section reviews past academic work on the subject of context awareness vulnerabilities within the scope of Bring Your Own Device (BYOD). The section covers critical analysis of context awareness vulnerabilities in BYOD environments, theoretical review focusing on context awareness vulnerabilities within BYOD framework, empirical review, conceptual framework and summary of research gaps.

2.2 Critical Review of Context Awareness in BYOD environments

2.2.1 Definition of context awareness

Context awareness, a term increasingly used in cyber-security and technology fields, refers to the capacity of systems or applications to detect, interpret, and respond to various contextual factors such as location, time, user activity, and device identity. According Wani et al.(2022), context awareness is defined as a system's ability to use context to provide relevant information or services to the user, where relevancy is dependent on the user's task. This definition highlights the role of context in tailoring user experiences and interactions with systems based on the environment. Another definition by Fernandez-Rojas et al.(2019)describe context awareness as the capability of systems to adapt their operations by sensing environmental contexts, such as who is using the device, what resources are nearby, and how the user is interacting with the system. This perspective emphasizes the system's ability to dynamically adjust its behaviour in response to environmental changes. Also, Augusto (2022) defined context awareness as a system's ability to adapt to the changing needs and situations of its users by utilizing contextual information like location, identity, time, and activity.

In the context of BYOD (Bring Your Own Device) environments, context awareness is essential for bolstering cyber-security measures. According to Rah (2023), it enables systems

to dynamically adjust security protocols based on the specific context in which personal devices are utilized, thereby ensuring more robust protection. Veljkovic and Budree (2019) suggest that context-aware security system can automatically escalate security measures when a device is accessed from a remote location or when it detects unusual activity patterns that deviate from the norm. This adaptive capability is crucial in mitigating risks associated with unauthorized access, data breaches, and other cyber threats that are prevalent in BYOD settings. By accurately interpreting and responding to the varied contexts in which devices are used, organizations can significantly enhance their overall cyber-security posture, making context awareness a critical component in managing modern BYOD environments effectively.

2.2.2 Context awareness in cyber-security

The relevance of context awareness to cyber-security cannot be overstated, particularly as Bring Your Own Device (BYOD) environments continue to gain traction in modern workplaces (Bada, Sasse & Nurse, 2019; Zwilling et al., 2022). In traditional security frameworks, static rules and predefined protocols have often been employed to protect sensitive information, however with increasing diversity of devices, operating systems, and usage scenarios that characterize BYOD environments has rendered these traditional measures inadequate (Renaud & Ophoff, 2021). As organizations allow employees use their personal devices, ranging from smartphones and tablets to laptops and wearables—for work-related tasks, the challenge of securing corporate data without compromising user convenience becomes more complex (Khader, Karam & Fares, 2021). This complexity arises from the varied contexts in which these devices are used, which traditional security models are ill-equipped to handle.

Context-aware security mechanisms present a solution by offering a dynamic and adaptive approach to safeguarding sensitive information (Zwilling et al., 2022). These mechanisms work by collecting and analysing contextual data—such as user behaviour, device

characteristics, and environmental factors—and then tailoring security responses accordingly. Systems set-up for context awareness, have capability to recognize when a device is being accessed from an unfamiliar location or during unusual hours and can adjust security protocols in real-time to mitigate potential risks (Renaud & Ophoff, 2021). This adaptive approach not only enhances the detection of potential threats but also reduces false positives, leading to more efficient and effective security management. False positives, where benign activities are flagged as suspicious, are a common issue in traditional security systems and can lead to unnecessary disruptions. By incorporating context awareness, security systems can more accurately differentiate between genuine threats and normal user behaviour, thereby improving both security and user experience (Khader et al. 2021).

In addition, context-aware security is particularly relevant in addressing specific threats associated with BYOD environments, such as unauthorized access, data leakage, and device loss or theft (Renaud & Ophoff, 2021). Since personal devices are used in various locations and often connected to multiple networks, the risk of exposure to malicious activities is higher. Context-aware systems can monitor these variables in real-time, providing heightened security when a device connects to a public Wi-Fi network or accesses sensitive corporate data from an unfamiliar location. This approach is also beneficial in preventing insider threats, where an employee with authorized access may inadvertently or intentionally compromise security (Bada et al., 2019). By continuously assessing the context in which data is accessed and used, organizations can implement more granular access controls, ensuring that sensitive information is only accessible under appropriate conditions.

2.2.3 Setbacks towards implementation of context-aware security

The leading setback towards implementation of context-aware security challenges is the accurate collection and interpretation of contextual data (Aldawood & Skinner, 2019). The diverse nature of devices used in BYOD settings—varying widely in terms of hardware,

software, and network capabilities—makes it difficult to standardize the data collection process (Zwilling et al., 2022). Each device may provide different types and amounts of data, complicating the task of creating a unified and comprehensive security strategy. Devices such as smartphone may offer precise GPS data, while a laptop may not have location tracking enabled, leading to gaps in context awareness (Bada et al., 2019). Additionally, the dynamic nature of context poses further challenges. Factors such as location, network conditions, and even user behaviour are constantly changing, necessitating real-time data processing and decision-making. This requirement for real-time analysis can strain system resources, particularly in large organizations with numerous devices to monitor (Espinha Gasiba, Lechner & Pinto-Albuquerque, 2020). The need for rapid data processing and response also introduces the risk of latency, where security decisions may be delayed, potentially leaving systems vulnerable to fast-moving threats. Moreover, the integration of context-aware security mechanisms with existing IT infrastructure can be complex, requiring significant investments in both technology and expertise.

Another significant setback is the challenge of ensuring user privacy while collecting contextual data (Zwilling et al., 2022). The effectiveness of context-aware security depends on the availability of accurate and detailed information about users' activities and environments. However, this level of data collection can be perceived as intrusive, leading to concerns about privacy and the potential misuse of personal information. Users may be reluctant to share data if they feel it could be used to monitor their activities outside of work, leading to resistance in adopting BYOD policies that rely on context-aware security (Noor et al., 2023). Balancing the need for security with respect for user privacy is, therefore, a delicate task. Organizations must ensure that their data collection practices are transparent, that users are informed about what data is being collected and how it will be used, and that robust measures are in place to protect this data from unauthorized access or misuse.

Moreover, the ethical implications of context-aware security must be carefully considered. Organizations need to develop clear policies that define the scope and limits of context data collection, ensuring that it is only used for legitimate security purposes and not for unjustified surveillance of employees (Aldawood & Skinner, 2019). In addition, regulatory compliance is another critical aspect, as organizations must adhere to data protection laws and regulations that govern the collection and use of personal information. Non-compliance could lead to legal repercussions and damage to the organization's reputation. The cost of implementing and maintaining context-aware security systems can be prohibitive for some organizations (Espinha Gasiba et al., 2020). Advanced analytics, real-time processing capabilities, and integration with existing IT infrastructure require substantial financial investment. Additionally, ongoing maintenance, updates, and the need for specialized personnel to manage these systems add to the overall cost. For smaller organizations or those with limited resources, these costs may be a significant barrier to adopting context-aware security measures.

2.2.4 BYOD in financial institutions and SACCOs

The adoption of Bring Your Own Device (BYOD) policies in financial institutions has gained significant traction, driven by a variety of strategic benefits that align with the evolving needs of the sector (Chigada & Daniels, 2021). In a highly competitive and fast-paced environment like finance, the ability to enhance employee productivity, reduce operational costs, and support work-life balance has become increasingly important. Financial institutions, including banks, credit unions, and SACCOs, have recognized that allowing employees to use their personal devices for work-related tasks can lead to substantial advantages in these areas. A fundamental driver of BYOD adoption in financial institutions is the flexibility it offers employees (Dalla, 2021). Integrating BYOD strategy, enables staff to work from virtually anywhere, accessing real-time data and responding to client needs promptly. This capability is

particularly valuable in the financial sector, where timely decision-making and customer responsiveness are critical to maintaining a competitive edge (Chigada & Daniels, 2021). Such stragey gives staff power to attend to client portfolios or market data on their personal smartphone or tablet, enabling facilitation of faster and more informed operational decisions during client interactions. This flexibility not only enhances individual productivity but also improves overall organizational efficiency.

Moreover, adoption and use of personal devices under a BYOD policy allows employees to work with tools they are already familiar with, thereby reducing the learning curve associated with adopting new technologies (Ofusori, 2019). When employees use their preferred devices, they can often complete tasks more efficiently, as they are accustomed to the device's interface, features, and functionality (Palanisamy, Norman, & Mat Kiah, 2022).This familiarity can lead to higher productivity levels and fewer technical support requests, further reducing the operational burden on the institution's IT department. Cost savings forms another scope of benefit in driving BYOD adoption in financial institutions. By allowing employees to use their own devices, organizations can reduce the need to invest in and maintain a large inventory of company-owned devices (Chigada & Daniels, 2021). This reduction in capital expenditure can be substantial, especially for large institutions with a considerable number of employees. Additionally, the ongoing maintenance and replacement costs associated with company-owned devices are minimized, as employees assume responsibility for the upkeep of their personal devices. These cost savings can be redirected to other critical areas of the business, such as technology upgrades or customer service improvements.

Employee satisfaction and retention are also positively impacted by the implementation of BYOD policies (Aguboshim et al., 2023). Allowing employees to use their personal devices for work supports a more flexible and balanced work environment, which is increasingly

valued in today's workforce. Employees appreciate the ability to seamlessly transition between work and personal tasks without the need to switch devices, making it easier to manage their work-life balance (Palanisamy et al., 2022). This flexibility can lead to higher job satisfaction, increased loyalty, and reduced turnover, which are particularly important in the financial sector, where retaining experienced and skilled employees is crucial for maintaining high service standards and continuity in client relationships.

However, the adoption of BYOD in financial institutions also comes with challenges, particularly in the areas of security and regulatory compliance (Ofusori, 2019). Financial institutions must ensure that robust security measures are in place to protect sensitive financial data accessed on personal devices. This includes implementing encryption, remote wipe capabilities, and strong authentication protocols to prevent unauthorized access. Additionally, organizations must navigate the complex regulatory landscape governing data protection in the financial sector, ensuring that BYOD policies comply with relevant laws and industry standards.

2.2.5 Unique cyber-security challenges in SACCOs and risks of BYOD

SACCOs, as financial cooperatives, face a distinct set of cyber-security challenges that set them apart from larger financial institutions (Sirma, Abeka & Okelo, 2019). One of the most significant challenges is the limited financial and technological resources available to SACCOs (Tambasi, 2019). Unlike larger banks that can afford to invest in state-of-the-art security technologies and maintain dedicated IT security teams, SACCOs often operate on tighter budgets. This financial constraint can severely limit their ability to implement and maintain advanced security measures, leaving them more susceptible to cyber-attacks. The reliance on outdated or inadequate security systems is a direct consequence of these limitations, making SACCOs more vulnerable to breaches and other cyber threats (Sirma et al., 2019). The integration of Bring Your Own Device (BYOD) policies within SACCOs adds another layer

of complexity to these cyber-security challenges (Aguboshim et al., 2023). Employees using personal devices for work-related tasks may not have the necessary security configurations, such as encryption, firewalls, or antivirus software that are critical for protecting against cyber threats. The decentralized control over these personal devices means that SACCOs often struggle to enforce consistent security policies across all endpoints. Without the ability to monitor and manage these devices effectively, SACCOs face heightened risks, as unauthorized access or data leaks can occur without the institution's knowledge.

Furthermore, the decentralized nature of SACCO operations, with branches often spread across various geographic locations, compounds these cyber-security risks (Sirma et al., 2019). Employees accessing sensitive data from remote or unsecured networks increase the likelihood of security breaches. The geographical spread of SACCO branches complicates the implementation of uniform security protocols, as different branches may face varying levels of threat and have different levels of security infrastructure (Tambasi, 2019). This inconsistency can create weak points within the organization's overall security framework, making SACCOs an attractive target for cybercriminals. Additionally, the lack of centralized IT governance and the potential for varying levels of employee cyber-security awareness across different branches can further increase the risks associated with BYOD. Employees in remote branches might not receive the same level of training or support as those in more central locations, leading to gaps in understanding and adherence to security protocols (Sirma et al., 2019). This unevenness in security awareness and practices can lead to vulnerabilities that cybercriminals can exploit.

2.3 Theoretical Framework

2.3.1 Risk-adaptable access control model

The Risk-Adaptable Access Control Model (RAdAC) is a significant development in the field of information security, particularly in dynamic environments where access decisions must consider varying levels of risk (Abdullah & Bakar, 2018). The model is credited to Dr. Ravi

Sandhu, a prominent figure in cyber-security, along with his colleagues, in 2000. Dr. Sandhu has made numerous contributions to access control models, such as the widely recognized Role-Based Access Control (RBAC) model. RAdAC emerged as a response to the limitations of traditional access control models, which typically enforce static rules and policies without accounting for the dynamic nature of risk in real-time environments (Mawla, Gupta & Sandhu, 2022).

The RAdAC model, submits that access control decisions should not be solely based on predefined roles or attributes but should dynamically adapt to the perceived risk level associated with a specific access request (Atlam et al., 2018). The model incorporates risk assessment as a core component of the decision-making process, allowing for more flexible and context-aware access control. The key premise of RAdAC is that security measures should balance the need for protection with the need for operational efficiency, adjusting access privileges based on the current risk context (Mawla et al., 2022). This adaptability is crucial in environments where the potential consequences of unauthorized access vary significantly depending on the situation.

Proponents of of the RAdAC submit claims that, the model offers flexibility in dealing with real-time changes in the threat landscape (Atlam et al., 2018;Khambhammettu et al., 2013). Unlike traditional models that operate on rigid rules, RAdAC can dynamically respond to evolving risks, making it well-suited for modern, fast-paced digital environments. In addition, the supportes of the model argue that RAdAC provides a more comprehensive approach to access control by considering not only the identity and role of the user but also the sensitivity of the resource and the context of the access request. This leads to more informed and precise access decisions. Further, Atlam et al.(2018) and Khambhammettu et al.(2013) claim that, the model has ability to reduce the operational burden on organizations by allowing

low-risk activities to proceed with minimal security checks, thereby improving efficiency while still maintaining high levels of security for more sensitive operations.

However, critics of the RAdAC model point to its complexity involved in implementing and managing a dynamic risk assessment system. According to Abdullah and Bakar (2018), notes that determining risk levels in real-time and adjusting access controls accordingly requires sophisticated algorithms and substantial computational resources, which can be challenging for organizations with limited technical capabilities. Additionally, the accuracy of risk assessments is a point of concern (Mawla et al., 2022). Critics argue that incorrect risk evaluations could either over-restrict access, hampering productivity, or under-restrict access, leading to potential security breaches. Another critique is that RAdAC relies heavily on accurate and up-to-date information about the environment, the user, and the resources, which may not always be readily available, especially in highly dynamic or decentralized environments.

The RAdAC model is applicable in the current study, whose context centers on context awareness vulnerabilities within BYOD environments for SACCOs in Kenya. The RAdAC model underpins the research by providing a framework for understanding how access control mechanisms can be adapted to the specific risks associated with BYOD practices. SACCOs, like many financial institutions, face unique security challenges due to the sensitive nature of the data they handle and the diverse range of devices used by employees under BYOD policies. The dynamic nature of RAdAC is particularly relevant in such a context, as it allows SACCOs to tailor their access control strategies based on real-time assessments of risk, considering factors such as device security, user behaviour, and the sensitivity of the accessed information. Through application of the principles of RAdAC, the study aims to explore how SACCOs can implement more effective and context-aware access control measures that address the specific vulnerabilities associated with BYOD environments. This approach aligns with the need for

SACCOs to balance security with operational efficiency, ensuring that employees can access necessary resources without compromising the organization's overall security posture. The RAdAC model thus provides a valuable theoretical foundation for developing adaptive security strategies that are responsive to the dynamic risks inherent in BYOD practices within the financial sector.

2.3.2 Activity theory

Activity Theory is a vast theoretical framework which emerged from the work of Russian psychologists Lev Vygotsky, Alexei Leontiev, and Sergei Rubinstein, with Vygotsky mostly credited as its founder and pioneer (Bradbury, Doe & Palmquist, 2022). The theory was initially proposed in the 1920s and 1930s, then was developed further by Leontiev in the 1940s and 1950s (Mironenko, 2020). Vygotsky's foundational ideas revolved around the concept that human cognition is deeply influenced by social interactions and cultural contexts. This theory is part of the broader framework of cultural-historical psychology, which posits that learning and development are inherently social processes, mediated by cultural tools and artifacts (Bradbury et al., 2022).

Activity Theory proposes that human activity is the fundamental unit of analysis when studying human behaviour and cognition (Taylor et al., 2019). According to the theory, activities are driven by needs and objectives, which are realized through interactions between individuals and their environment (Mironenko, 2020). These interactions are mediated by tools, rules, community, and the division of labor, all of which shape the way activities are carried out. The theory emphasizes the contextual and dynamic nature of human actions, suggesting that cognition cannot be fully understood without considering the social, cultural, and historical context in which it occurs (Yasnitsky, 2019).

Proponents of Activity theory commonly cite several key points in favor of its comprehensive and holistic approach to understanding human behaviour. Taylor et al. (2019)

postulated that activity theory wielded ability to integrate individual and social factors in the analysis of human activities, offering a more nuanced understanding of how people interact with their environment. Unlike theories that focus solely on individual cognition, Activity Theory considers the broader context, including the tools and artifacts people use, the social rules that govern behaviour, and the roles and responsibilities within a community. Further, it's viewed that the activity theory is highly adaptable, capable of being applied to a wide range of disciplines, including education, psychology, organizational studies, and human-computer interaction (Mironenko, 2020). Its flexibility allows for the examination of complex systems and processes, making it a valuable tool for researchers across various fields. In addition, the theory is favourably viewed for its emphasis on the transformative potential of human activities. By focusing on how individuals and groups can change their practices and environments, the theory offers insights into processes of learning, development, and innovation.

On the aspect of critique to activity theory, Yasnitsky(2019) notes that the model is viewed as complex and abstract in nature, which can make it difficult to apply in practical research settings. The theory's emphasis on the interplay of multiple factors, such as tools, rules, and community, can result in a level of complexity that some researchers find challenging to operationalize. Additionally, another criticism on the theory, is lack to specificity in explaining individual cognitive processes, as its broad focus on social and contextual factors can sometimes overshadow the role of individual agency and decision-making. Also, the theory's roots in Marxist ideology have been viewed as a limiting factor for its applicability in non-collectivist cultures, where individualism is more prominent.

Activity theory is relevant in the current study, which centres on context awareness vulnerabilities in BYOD environments within SACCOs in Kenya, as it proposes a valuable framework for understanding how employees interact with their devices and the organizational

environment. The BYOD practice involves employees using their personal devices for work-related activities, which inherently blurs the lines between personal and professional contexts. Activity theory's emphases on dynamic interaction between individuals, tools, and their environment is particularly relevant in this setting, as it allows for a deeper exploration of how these interactions influence security behaviours and practices. The theory links with the current study by examining how employees' activities within a BYOD environment are shaped by various factors, including organizational policies, technological tools, and social norms. Understanding these interactions can help identify potential vulnerabilities in the context awareness of employees, particularly in how they perceive and manage security risks while using their personal devices for work. The theory underpins the study by offering a comprehensive lens through which to examine the complex, multi-layered nature of BYOD practices, ultimately contributing to the development of more effective strategies for mitigating context-aware security vulnerabilities in SACCOs.

2.3.3 Technology acceptance model

The Technology Acceptance Model (TAM) is credited to Fred Davis, which He proposed as part of His Doctoral Dissertation at the Massachusetts Institute of Technology (MIT) in 1986 (Malatji, Eck & Zuva, 2020; Natasia, Wiranti & Parastika, 2022). The TAM theory is a widely applied theoretical framework in technology studies which seek to detail, how and why individuals adopt and use technology (Guner & Acarturk, 2020). Davis proposed TAM as an adaptation of Ajzen and Fishbein's Theory of Reasoned Action (TRA), aiming to better understand user behaviour in the context of technology acceptance and use. The TAM theory submits that two primary factors determine an individual's intention to use a particular technology, which are the Perceived Usefulness (PU) and the Perceived Ease of Use (PEOU) (Guner & Acarturk, 2020). Perceived Usefulness is defined as the degree to which a person believes that using a specific system would enhance their job performance. Perceived Ease of

Use refers to the extent to which a person believes that using the system would be free of effort. According to TAM, if a technology is perceived as useful and easy to use, individuals are more likely to adopt it (Opoku & Enu-Kwesi, 2019). These perceptions, in turn, influence the user's attitude toward using the technology, which directly affects their behavioural intention to use it, and ultimately, their actual use of the technology.

A significant portion of TAM proponents, argue that TAM is simple and easy to use. According to Guner and Acarturk(2020), the TAM's straightforward structure, focusing on two key constructs of perceived usefulness and perceived ease of use, makes it relatively easy to apply across various contexts and different types of technologies. This simplicity allows researchers and practitioners to quickly assess the likelihood of technology adoption within organizations or among users. Further, TAM is vastly cited through numerous studies across different domains, including information systems, healthcare, education, and e-commerce. Opoku and Enu-Kwesi (2019) observed that, TAM's robustness and predictive power has made it a foundational model for understanding user acceptance of technology. The TAM's adaptability is another key factor of its popularity, as the model has been extended and modified to include additional variables, such as perceived enjoyment, subjective norms, and perceived risk, allowing it to address the specific needs of different research contexts.

Main criticism for the technology acceptance model is the view that it oversimplifies the complex process of technology adoption. According to Malatji et al., (2020) note that focusing primarily on perceived usefulness and perceived ease of use, TAM overlooks other important factors that can influence technology acceptance, such as social influence, cultural context, and individual differences. Additionally, some researchers have questioned the model's applicability in contexts where the technology in question is mandatory rather than voluntary. In such cases, users may adopt the technology not because they find it useful or easy to use, but because they have no choice. Another critique is that TAM does not adequately

address the post-adoption phase, where factors like user satisfaction, continued use, and technology impact become more relevant.

The technology acceptance model is applicable in the current study, in that within the scope of context awareness vulnerabilities in BYOD environments within SACCOs in Kenya, the theory provides a useful framework for understanding how employees perceive and interact with BYOD policies and security technologies. The study seeks to explore how the perceived usefulness and ease of use of security measures, such as mobile device management (MDM) software or multi-factor authentication, influence employees' willingness to comply with security protocols and adopt safe practices while using their personal devices for work. Through adoption of TAM foundation, the study identifies potential barriers to the effective implementation of BYOD security measures in SACCOs. Instance such as, employees' perception of security protocols as cumbersome or not directly beneficial to their work, presents a likelihood of ignoring them, increasing the risk of context-aware vulnerabilities. Understanding these perceptions can help organizations design more user-friendly security policies that align with employees' needs and work habits, ultimately enhancing the overall security of the BYOD environment. In this way, TAM underpins the study by offering insights into the factors that drive or hinder technology adoption and compliance, contributing to the development of more effective strategies for managing security risks in SACCOs.

2.3.4 Rational choice theory

Rational Choice Theory (RCT) is credited to the works of John von Neumann and Oskar Morgenstern who, in 1944, laid the foundation for its application in decision-making processes through their work on game theory in "Theory of Games and Economic Behaviour" (Asikhia, Osinowo & Kassim, 2021; Ostrom, 2019). The rational choice theory posits that individuals make decisions by rationally weighing the costs and benefits to maximize personal advantage

(Hudik, 2019). It assumes that individuals have stable preferences and are fully informed, making choices that will provide them with the highest utility.

In technology studies, the rational choice model is applicable and relevant as it explains how individuals or organizations adopt new technologies based on perceived benefits versus potential costs (Blossfeld & Prein, 2019). In the subject Bring Your Own Device (BYOD) practices adaptability within organizations, employees and employers might weigh the benefits of flexibility, convenience, and cost savings against the risks of security breaches, data loss, and potential privacy issues. The model, helps in understanding these decisions, providing framework to analyse why certain security measures are adopted or ignored based on the perceived trade-offs (Asikhia et al., 2021).

The rational choice model is applicable in the current study. The focus of the study centers on context awareness vulnerabilities within BYOD environments in large SACCOs in Kenya. The model is relevant as it explains the decision-making processes of SACCO employees and management when it comes to using personal devices for work purposes. It offers insights into how individuals rationalize their actions regarding security practices and the adoption of BYOD policies. The theory helps to explore the reasons behind the potential negligence or non-compliance with security protocols, as users might weigh the immediate convenience of using personal devices against the less tangible risks of data breaches or other security threats. This understanding is crucial for developing strategies that align security practices with the rational choices of individuals within the organization.

2.4 Empirical Review

The subject of BYOD has emerged as a key strategy for integration in modern day corporate scene, thus it has equally attracted interest from scholars across globe. This section looks into some already published studies and academic work centering on the subject of BYOD and its

implications in area of cyber-security and existing risks in purview of context awareness vulnerabilities.

2.4.1 Access time and context awareness vulnerability in BYOD environments

Studies by Lopes, Lousã, and Almeida (2023) and Maseko (2023) offered insight on the role of access time in expounding context awareness vulnerability in BYOD environment. Lopes et al. (2023) explores on the challenges of Information Security Management (ISM) in micro-companies within the information technology sector. The research aimed to identify the primary risks associated with ISM in these small enterprises.

The study employed a qualitative approach, conducting four case studies of micro-companies. The findings revealed that while these companies recognize the importance of information security due to increasing external threats, they struggle with a lack of commitment, resources, and knowledge, which impedes the effective implementation of ISM policies. The study identified that inconsistent security practices during off-peak times in micro-companies led to vulnerabilities, highlighting the role of access time.

The gap identified in relation to the current study on context awareness vulnerabilities in BYOD environments for SACCOs in Kenya is that while Lopes et al. focus on ISM challenges in micro-companies, the current research seeks to address specific vulnerabilities related to BYOD practices in a financial sector context, with a focus on SACCOs.

Maseko's (2023) study addresses the rising security vulnerabilities in financial institutions due to increased digitization, particularly during the COVID-19 pandemic when teleworking became prevalent. The study focuses on phishing attacks and aims to provide solutions to reduce user susceptibility to such threats.

A qualitative approach was employed, utilizing semi-structured interviews and thematic analysis to identify patterns and commonalities in participants' responses. The research was grounded in the Routine Activity and Rational Choice theories, which explain the

conditions necessary for crimes like phishing to occur and the motivations behind offenders' choices. The study found that users often neglect established security protocols, increasing the risk of successful phishing attempts.

The recommendations emphasize human-centric approaches, highlighting the importance of close collaboration between employees and IT personnel to mitigate phishing risks. The study showed that users often neglect security protocols during non-standard working hours, increasing susceptibility to threats, which highlights the relevance of access time in regard to vulnerability context. The gap in relation to the current study lies in Maseko's focus on phishing, whereas the current research investigates context awareness vulnerabilities in BYOD environments for SACCOs in Kenya.

Both Lopes et al. (2023) and Maseko (2023) reveal that irregular access times elevate security risks, but no study specifically examines the role of access time in SACCO environments, a gap this study aims to address.

2.4.2 Device Usage and Context awareness vulnerability in BYOD environments

Studies by Almarhabi, Alghamdi, and Bahaddad (2022), Annansingh (2020) and Sikder et al. (2021) present an insight on the connection of device usage and context awareness vulnerabilities in BYOD environments. Almarhabi et al. (2022) conducted a study to explore the Bring Your Own Device (BYOD) trend in Saudi Arabia's health sector, focusing on its benefits and associated cyber-security risks. The study aimed to assess the current understanding, usage, and challenges of BYOD within this sector.

A quantitative research methodology was employed, using a structured survey divided into three components: demographic information, personal device usage for work, and BYOD awareness. Participants' opinions were gauged using a Likert scale, and data were analysed using various software tools. The findings revealed that while BYOD offers numerous benefits, such as increased flexibility and employee satisfaction, it also poses significant risks, including

vulnerability to malware, data breaches, and legal issues. The study emphasized the need for increased employee awareness and robust policies to mitigate these risks.

Almarhabi et al. (ibid) found that found that personal device usage in Saudi Arabia's healthcare sector creates vulnerabilities, including malware attacks and data breaches. However, the research did not specifically address context awareness vulnerabilities within BYOD environments, a critical aspect that the current study will investigate in the context of SACCOs in Kenya.

Annansingh (2020) examines the cyber-security risks associated with young professionals using personal mobile devices for work, contributing to increased exposure to cyber-attacks and knowledge leakage. The study employed a mixed-method approach, using survey questionnaires to gather insights from millennia's and conducting interviews with security personnel.

The data analysis included descriptive analysis and open coding. The findings revealed that young professionals, prioritize convenience and access to technology over security concerns, viewing the use of personal devices as a right. The study also highlighted the need for organizations to enhance and enforce BYOD policies to mitigate security risks and knowledge leakage. The study show that in regard to device usage, young professionals prioritized convenience over security, increasing device usage risks. The gap identified in this study, compared to the current research on context awareness vulnerabilities in SACCOs in Kenya, is that while Annansingh focuses on generational attitudes and general organizational risks, the current study seeks to address specific context-aware vulnerabilities in the financial services sector, particularly SACCOs.

Sikder et al. (2021) looked into the security vulnerabilities associated with smart devices, focusing particularly on sensor-based threats and attacks. The research aimed to

explore how attackers exploit sensors like accelerometers, gyroscopes, and microphones to compromise device security, transfer malware, or trigger malicious activities.

The methodology involved a comprehensive survey of existing sensor-based threats and a detailed analysis of countermeasures developed to secure smart devices from such vulnerabilities. Findings showed that critical security risks posed by sensors in smart devices, which lack adequate security mechanisms to control sensor usage by apps. The study shows how attackers exploit sensors in smart devices, such as accelerometers and gyroscopes, to compromise security, revealing gaps in app-level sensor security, pointing to connection between device usage and enhanced exposure to vulnerabilities.

However, the study primarily addresses general security issues in smart devices and does not delve into the specific context of BYOD environments in financial institutions, such as SACCOs in Kenya. This presents a research gap, as the current study aims to explore context awareness vulnerabilities in BYOD environments, focusing on large SACCOs, which have unique security challenges.

The studies by Almarhabi et al. (2022), Annansingh (2020) and Sikder et al. (2021) focused on general device risks rather than usage patterns in SACCO BYOD settings. Our study addresses this gap by analyzing how device usage influences vulnerability within SACCOs.

2.4.3 Location and context Awareness Vulnerability in BYOD environments

Studies by Downer and Bhattacharya (2022) and, Moeketsi, Adeyelure, and Segooa (2024), puts into context the relationship between location and vulnerability in BYOD environments. Downer and Bhattacharya (2022) explored BYOD security mechanisms within Australian organizations, focusing on how employees practice and perceive these mechanisms. The study, driven by the surge in BYOD adoption during the COVID-19 pandemic, aimed to understand

employee interactions with security frameworks and identify vulnerabilities in business IT networks.

Utilizing a quantitative approach, the researchers conducted an online survey distributed through social media and professional networks. The survey, hosted on Survey-Monkey, collected data on employees' experiences and knowledge regarding BYOD security. Key findings revealed that while 90% of employees used default security features, only 40% of businesses enforced formal BYOD-specific policies. The findings show that Australian businesses faced unique threats during remote work due to poor enforcement of location-based access controls.

The study highlighted that network access controls and antimalware were common security measures, but there was a notable gap in written policies and clear boundaries between work and personal applications. This study's gap relates to its focus on Australian businesses, whereas the current research on context awareness vulnerability in BYOD environments for SACCOs in Kenya will address how local context and sector-specific needs influence BYOD security practices and perceptions.

Moeketsi et al. (2024) study looked into the integration of BYOD (Bring Your Own Device) practices in the South African healthcare sector, focusing on the development of an information-security assessment model.

The research targeted the private healthcare sector in Gauteng Province, utilizing a sample size of 128 respondents. The study employed a closed-ended questionnaire analyzed using SPSS version 28, validated through expert judgment. The findings established that training, security threats, and security controls significantly contribute to the development of the BYOD security assessment model. The study showed how security threats vary by location, with healthcare providers in Gauteng Province facing specific challenges in BYOD adoption, thus linking location and vulnerabilities.

Despite its comprehensive approach, the study primarily focuses on healthcare and does not address the unique context awareness vulnerabilities in the financial sector, particularly within SACCOs in Kenya. This gap underlines the need for further research to explore and develop context-specific security models for BYOD environments within SACCOs, ensuring that they address the distinct challenges posed by such institutions.

Both Downer and Bhattacharya (2022) and Moeketsi et al. (2024), highlight the role of location in regard to exposure to vulnerabilities. Despite these insights, prior studies overlook location-specific vulnerabilities in SACCO environments. The current study examined how access location influences security, particularly focusing on context-aware threats in Kenyan SACCOs to address this significant gap.

2.4.4 Role Risk factor and context awareness vulnerability in BYOD environments

Studies by Kholoanyane's (2020), Kreeft and Govender (2022), and Muthuswamy (2023) present a nexus between the aspect of roles risk factor and vulnerabilities in BYOD environments. Kholoanyane's (2020) study explores the challenges and importance of training and security awareness in the context of BYOD (Bring Your Own Device) among South African SMEs. The research aims to develop a guideline for effective BYOD security training and awareness policies, focusing on the human element as a critical factor in security risks.

The study employed a qualitative methodology, utilizing extensive literature reviews, in-depth interviews, and surveys with IT and security personnel to gather insights. The study established that SMEs are aware of BYOD security risks but often lack formal policies and sufficient management support, leading to inadequate employee engagement in security practices. The study determined that inadequate employee training and support exacerbated security risks.

The study emphasizes the necessity of tailored, adaptable training and awareness policies to minimize risks, noting that human error is the most significant vulnerability. The

gap in relation to the current study is that Kholoanyane's research focuses on SMEs in South Africa, whereas the current study investigates context awareness vulnerabilities in BYOD environments specifically for SACCOs in Kenya, requiring a more focused approach on context-specific vulnerabilities.

Kreeft and Govender (2022) looked into the security risks associated with BYOD practices within South African SMEs, focusing on whether these organizations have BYOD policies and the awareness of security risks among management and employees.

The study utilized descriptive research and stratified random sampling to survey 27 SME owner-managers and ninety-four employees, with the data collected through online questionnaires. Results who that there existed a high level of security risk awareness among SMEs; however, most organizations lacked a formal BYOD policy, leaving them vulnerable to IT security threats. Additionally, no significant relationship was found between security risk awareness and BYOD policy non-compliance behaviour. Findings showed SME employees without formal BYOD policies face heightened risks despite high awareness levels.

This study highlights a gap in understanding why organizations with high awareness of security risks delay implementing BYOD policies. In contrast, the current study focuses on context awareness vulnerabilities within the BYOD environment in SACCOs in Kenya, emphasizing the need to explore context-specific risks in financial institutions rather than SMEs.

Muthuswamy (2023) conducted a qualitative study to investigate cyber-security challenges in Saudi Arabia's digital workplace, focusing on employee experiences in various organizations. The study aimed to identify key cyber-security threats, including lack of awareness and training, insider risks, social engineering attacks, poor password practices, and BYOD (Bring Your Own Device) issues.

Data were collected from 20 participants through semi-structured interviews, and thematic analysis was used to identify significant themes. The study found that insufficient cyber-security awareness and training, along with the rise of BYOD practices, contribute to increased risks within digital workplaces. These insights stress the need for robust cyber-security measures and continuous training programs. The study found that insider threats and poor password practices are critical risks linked to employee roles in digital workplaces.

However, the study did not specifically explore context awareness vulnerabilities, a critical gap that the current study seeks to address. The focus will be on understanding these vulnerabilities within BYOD environments in SACCOs in Kenya, providing targeted insights for improving cyber-security in this specific context.

Submissions by Kholoanyane's (2020), Kreeft and Govender (2022), and Muthuswamy (2023) do not address role-specific vulnerabilities within SACCOs. The current study bridges the gap by exploring how role-based access and risk factors contribute to context-aware vulnerabilities in SACCO BYOD environments.

2.6 Machine Learning Models in BYOD Environments

2.6.1 Utilization of xtreme gradient boosting (XGBoost) in anonaly detection

An analysis by Balega et al. (2024) explored on the optimization of anomaly detection for internet of things (IOT) and BYOD environments using machine learning (ML) models. The study addresses the critical need for efficient and effective anomaly detection, a cornerstone of securing IOT networks and personal devices in active use and operational environments. The researchers evaluated Extreme Gradient Boosting (XGBoost), Support Vector Machines (SVMs), and Deep Convolutional Neural Networks (DCNNs) across three datasets—IoT-23, NSL-KDD, and TON-IOT and a real-world IOT test bed.

For the three models, XGBoost achieved better scores than other models recording an accuracy of (99.98%) and demonstrated superior computational efficiency, training 717.75

times faster than SVM and significantly faster than DCNN. The findings underscore XG-Boost's robustness for anomaly detection in IOT and BYOD contexts. A primary limitation lies in the study's dependence on specific datasets, which may not fully capture the diversity of IOT anomalies. Future research should explore more diverse environments to generalize the model's applicability.

The analysis, shows that XGBoost outperforms linear regression in complex anomaly detection, offering higher accuracy (99.98%) and superior computational efficiency. However, unlike linear regression, which provides transparent, interpretable relationships between variables, the XGBoost model operates as a black-box model, which in SACCO setting will make it difficult to derive actionable insights on BYOD vulnerabilities. Additionally, the XGBoost model relies heavily on specific datasets, limiting its adaptability to diverse SACCO environments where context-aware security risks vary in range. In contrast, the linear regression enables quantifiable risk assessments based on access time, location level, and role risk factor, making it more practical and policy-driven for SACCO security improvements.

2.6.2 Application of machine learning models in detection of malware threats

A model developed by Chizoba and Kyari (2020) was conceptualized to enable the detection of Advanced Persistent Threats (APTs), a sophisticated class of malware, in environments influenced by technological advancements such as Industry 4.0 and BYOD. The study identified challenges such as poor understanding of APT tactics and inefficient network traffic log analysis, which hinder effective threat detection. To examine these underlying pitfalls, the researchers utilized an ensemble of classifiers, including Support Vector Machine (SVM), Random Forest (RF), and Decision Tree, combined with majority voting to enhance detection accuracy. Through a simulation of APT attacks in a virtual environment and using dimensionality reduction techniques on network traffic logs, they improved log processing and detection. The ensemble model achieved an impressive detection accuracy of 90.47%, with the

Random Forest model performing best in the majority voting process. The model however relied on simulated and specific datasets which limits its applicability to diverse real-world BYOD scenarios, requiring further validation in broader environments.

Chizoba and Kyari's, model which integrates integrating SVM, Random Forest, and Decision Tree, was found to enhance APT detection with 90.47% accuracy through majority voting. Whereas the model presents desirable effective levels for cyber-security, these models require high deployment of computational resources and extensive network log data, making them less practical for SACCOs with limited IT infrastructure. In linear regression model, a simplified approach is provided to interpretable relationships between access factors and vulnerability risks, for which the ensemble models lack explain-ability. In addition, the ensemble model relies on use of simulated datasets, thus limiting real-world applicability, whereas linear regression enables context-driven security insights for SACCO BYOD environments.

2.6.3 Combination of machine learning methods in anomaly detection in environments like BYOD

Munuo (2024) examined the application of Zero Trust Architecture (ZTA) to enhance the protection of Personally Identifiable Information (PII) in the financial services sector, especially in environments like BYOD. The study integrates machine learning (ML) models, including Logistic Regression, Random Forest, XGBoost, and Time Series Analysis, to strengthen anomaly detection capabilities within ZTA systems. Within the BYOD settings, ZTA model transfers security focus from network perimeters to users, devices, and applications, which then ensures continuous authentication and dynamic trust establishment. For the models employed, XGBoost emerged as the most effective algorithm, excelling in accuracy and F-measure metrics for anomaly detection. The research also highlights that incorporating more data sets can marginally improve anomaly detection. The study's primary

limitation is the simplicity of the experimental architecture, which constrained the analysis of diverse intrusion types and influenced precision and recall outcomes. Through expanding the architecture and datasets would enhance generalizability and enhance detection capabilities.

Munuo, employed XGBoost, Random Forest, and Logistic Regression within Zero Trust Architecture (ZTA) for anomaly detection, emphasizing continuous authentication in BYOD environments. In the analysis, XGBoost attained high levels in accuracy, however its scalability requires high computational power and subsequently lacks interpretability, in comparison to linear regression, which enables transparent, quantifiable risk assessments. Munuo study, is limited in experimental architecture, which then constrains real-world applicability. In the context of SACCOs, where resource constraints and context-aware vulnerabilities matter, linear regression offers a simpler, cost-effective approach, enabling clear policy-driven decisions for BYOD security without reliance of excessive computational requirements.

2.6.4 Application of machine learning models in vulnerability scanner for sql injection in BYOD environments

Ussatova et al. (2023) conducted an analysis which focused on developing a vulnerability threat detection scanner using machine learning (ML) models to secure information systems within contexts such as BYOD environment and mobile utilization of resources. The research explored on vulnerabilities, particularly SQL injection threats, as critical risks to web services, networks, and operational systems. The scanner integrates ML models such as Naïve Bayes, Logistic Regression, Decision Tree, Random Forest, and XGBoost to classify and detect vulnerabilities effectively. In a Bring Your Own Device (BYOD) environment, such models are vital for identifying diverse security threats. The study emphasizes preprocessing steps like data cleaning, normalization, and feature extraction to train the models. The ML models achieved high performance metrics, which included accuracy, precision, Recall and F1-score,

demonstrating their effectiveness in identifying SQL injection threats. Despite these results, the study's main limitation is its narrow focus on SQL injections, leaving other potential BYOD vulnerabilities, such as unauthorized device access, not well captured. By integrating additional threats could enhance the scanner's utility.

Ussatova et al., utilized Naïve Bayes, Logistic Regression, Decision Tree, Random Forest, and XGBoost to develop a vulnerability scanner for SQL injection threats in BYOD environments. In practical application, these ML models excel in classification accuracy, however they require extensive preprocessing and computational power, making them less feasible within context where resources are limited, such as SACCOs. In comparison, linear regression models provide interpretable, quantifiable insights on access-level, related risks. Ussatova et al., study focuses on SQL injection, which overlooks broader BYOD vulnerabilities like unauthorized access. Thus, in regard to context-awareness, linear regression approach extends a simpler, actionable security solution, which can be scaled to institutions like SACCOs, in management of BYOD risks.

2.6.5 Application of machine learning models in an intelligent risk management framework

The study by Shah and Shankarappa (2018) introduces an intelligent risk management framework tailored for the Bring Your Own Device (BYOD) environment, addressing the shortcomings of traditional risk management systems. These systems often fail to counteract the complex threats posed by mobile devices in business networks, such as privacy breaches and data leakage. The proposed framework utilizes Machine Learning (ML) models, including Support Vector Machines (SVM), Multilayer Perceptron (MLP), Bayesian Networks (BN), and Random Forest (RF), to analyses Mobile Device Management (MDM) log files. These algorithms proactively detect potential risks in real time, enabling timely preventive measures. SVM emerged as the most effective algorithm, demonstrating high performance accuracy, low

false positives, and minimal true negatives, making it particularly reliable in the BYOD context. The study is however limited on its reliance on MDM logs, which may not capture all aspects of BYOD vulnerabilities.

Shah and Shankarappa, study utilized SVM, MLP, Bayesian Networks, and Random Forest for real-time BYOD risk detection via Mobile Device Management (MDM) logs. Application of SVM model returned high accuracy. However, these ML models require utilization of complex data processing frameworks which rely on MDM logs, which may not capture all BYOD vulnerabilities, notably the unauthorized access-level risks. In contrast, the Linear regression model, presents transparent, quantifiable insights into context awareness vulnerabilities, such as access time and role risk factor, making it a simpler, data-driven solution for SACCOs, which have limited IT resources.

TABLE 1. Summary of the Machine Learning Models

Authors/ Researchers	Focus of the Study	ML Model used	Findings	Limitations of the Model
Balega et al. (2024)	optimization of anomaly detection for internet of things (IOT) and BYOD environments using machine learning (ML) models	Extreme gradient boosting, Support Vector Machines, Deep Convolutional Neural Networks (DCNNs)	XGBoost achieved better scores than other models recording an accuracy of (99.98%) and demonstrated superior computational efficiency, training 717.75 times faster than SVM and significantly faster than DCNN.	Dependence on specific datasets, which may not fully capture the diversity of IOT anomalies.
Chizoba and Kyari (2020)	detection of Advanced Persistent Threats (APTs) in BYOD environments	Support Vector Machine, Random Forest and Decision Tree	The ensemble model achieved an impressive detection accuracy of 90.47%,	Model however relied on simulated and specific datasets which limits its applicability to diverse real-world BYOD scenarios
Munuo (2024)	Application of Zero Trust Architecture (ZTA) to enhance the protection of Personally Identifiable Information (PII) in the financial services sector	Logistic Regression, Random Forest, XGBoost, and Time Series Analysis,	XGBoost emerged as the most effective algorithm, excelling in accuracy and F-measure metrics for anomaly detection	Simplicity of the experimental architecture, which constrained the analysis of diverse intrusion types and influenced precision and recall outcomes.
Ussatova et al. (2023)	Development of a vulnerability threat detection scanner using machine learning (ML) models to secure information systems within contexts such as BYOD	Naïve Bayes, Logistic Regression, Decision Tree, Random Forest, and XGBoost	All models achieved high performance metrics, which included accuracy, precision, Recall and F1-score, demonstrating their effectiveness in identifying SQL injection threats	Has narrow focus on SQL injections, leaving other potential BYOD vulnerabilities, such as unauthorized device access not accounted for
Shah and Shankarappa (2018)	Assessment of intelligent risk management framework tailored for the Bring Your Own Device (BYOD) environment	Support Vector Machines (SVM), Multilayer Perceptron (MLP), Bayesian Networks (BN), and Random Forest (RF)	SVM was most effectives and the algorithms were able to detect potential risks in real time, enabling timely preventive measures	Relies on MDM logs, which may not capture all aspects of BYOD vulnerabilities

2.5 Conceptual Framework

A conceptual framework is a demonstration of link between independent variables and the dependent variable. The current study, seeks to examine context awareness vulnerabilities within BYOD environments. The independent variables for study include; access time, device usage, location and role risk-factor. The dependent vulnerability factor with indicators including; unauthorized access, data breaches, malware incidents and phishing attacks.

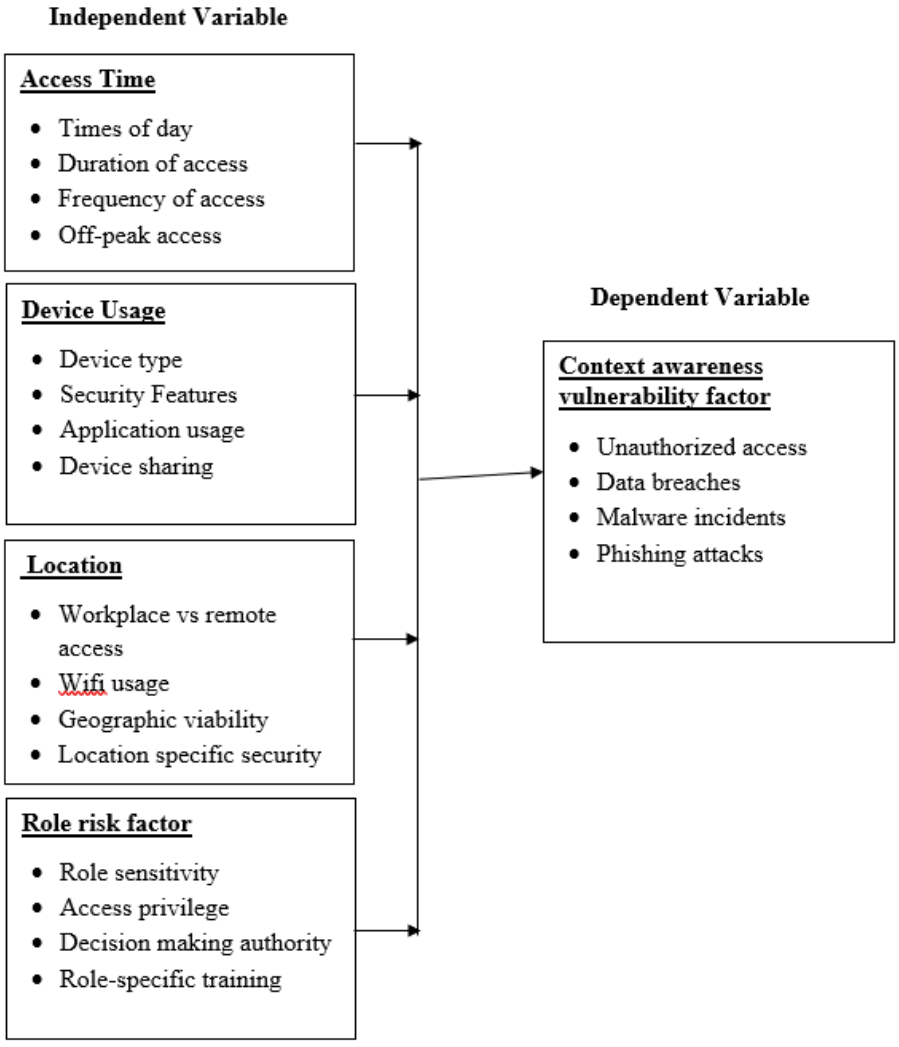


FIGURE 1. Conceptual Framework

Access Time: This refers to when employees access SACCO systems using their personal devices. Different access times could correlate with varying levels of vulnerability, depending on factors such as network security during off-peak hours.

Device Usage: This encompasses how employees use their personal devices for work, including the types of tasks they perform and the security of the devices. Higher usage of devices in unsecured environments may increase vulnerabilities.

Location Changes: The context in which the device is used, such as whether it is being used within the SACCO premises or in remote locations, can affect the security level. More frequent location changes can introduce more exposure to vulnerabilities.

Role Risk Factor: Employees' roles within the SACCO might determine their level of access to sensitive information, thus affecting the risk of vulnerability. For instance, higher-level employees with more access might present a greater risk if their devices are compromised.

Each of these independent variables can influence the level of context awareness vulnerabilities in a BYOD environment. Understanding how these variables interact can help SACCOs develop better strategies for mitigating risks associated with the use of personal devices in the workplace.

2.6 Summary of Research Gaps

Annansingh (2020) focused on generational attitudes towards BYOD and general organizational risks, but lacks exploration of specific context-aware vulnerabilities in the financial services sector, particularly within SACCOs in Kenya. Kreeft and Govender (2022) examined BYOD security risks in South African SMEs but does not address context-specific vulnerabilities in the financial sector, highlighting the need for sector-specific research, such as within SACCOs.

Sikder et al. (2021) investigated sensor-based threats in smart devices without delving into the context of BYOD environments in financial institutions, presenting a gap for research on context-aware vulnerabilities in SACCOs. Moeketsi, Adeyelure, and Segooa (2024) developed a BYOD security assessment model for South African healthcare but does not address vulnerabilities unique to the financial sector, particularly SACCOs in Kenya, necessitating context-specific research in this area.

Kholoanyane (2020) focuses on BYOD training and awareness in South African SMEs, yet does not investigate context-specific vulnerabilities within SACCOs, pointing to the need for targeted research in financial institutions. Lopes et al. (2023) addresses ISM challenges in micro-companies without focusing on BYOD vulnerabilities in financial institutions, emphasizing the need for context-specific research in SACCOs.

Aguboshim et al. (2023) provides a broad review of BYOD risks and policies but lacks focus on context-specific vulnerabilities within SACCOs, highlighting a need for targeted research in this financial sector. Downer and Bhattacharya (2022) explored BYOD security mechanisms in Australian organizations but does not address local context and sector-specific needs in SACCOs in Kenya, underlining the importance of local and sector-specific research.

Maseko (2023) investigated phishing attacks and user susceptibility but does not cover context-aware vulnerabilities in BYOD environments, particularly within SACCOs, emphasizing the need for sector-focused research. Ferdousi (2022) reviewed general BYOD cyber-security threats and strategies but does not specifically address context-aware vulnerabilities within SACCOs, underscoring the need for detailed research in this financial sector.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This study sought to investigate the risk factor towards context vulnerabilities within BYOD environment using linear regression technique for large SACCOs in Kenya. The study utilized primary data which was obtained from a leading large SACCOs in Kenya. This section of the study lays down the procedure and processes that was used to collect data needed for the study.

3.2 Research Design

Research design is the overall strategy or blueprint that outlines how a study is conducted, including the methods and procedures used to collect and analyze data (Mcleod, 2023). It provides a framework for addressing research questions or hypotheses, ensuring that the study is systematically organized and scientifically valid. The current study utilized a descriptive survey technique, employing a pre-set questionnaire tool to collect data from SACCO employees. The survey technique was particularly convenient for this study as it allowed for the systematic collection of data from a large sample, enabling a comprehensive evaluation of SACCO employees' device usage behaviours when conducting their daily operations within company precincts.

By using a descriptive survey, the study captured a wide range of responses, providing detailed insights into the patterns and practices associated with BYOD environments. A descriptive survey research design specifically involves collecting quantitative or qualitative data from a sample to describe and interpret characteristics, behaviours, or opinions of a population (Osuagwu, 2020). This design often uses structured questionnaires or interviews to gather information, allowing researchers to systematically explore and present findings on a given topic without manipulating variables. It is particularly useful for understanding current conditions, trends, or relationships within a population. This approach was especially useful

towards the identification of context awareness vulnerabilities, as it enabled the collection of data on various factors including; access times, device types, usage locations, and the roles of employees within the organization.

The structured nature of the questionnaire ensured that the data collected was both consistent and comparable across different respondents, facilitating accurate analysis and interpretation. Additionally, the descriptive survey allowed exploration of correlations between employee behaviours and potential security risks, making it an effective method for gathering the information needed to develop a predictive model for context awareness vulnerabilities. This method's flexibility and broad applicability made it well-suited for the study's objectives, ensuring that the data gathered was relevant and actionable for enhancing cyber-security in SACCOs' BYOD environments.

3.3 Target Population

The target population of a study refers to the entire group of individuals or entities that share common characteristics and from which the researcher intends to draw conclusions or make generalizations (Sallis *et el.*, 2021).The target population for this study comprised all employees of Mwalimu National SACCO who are based at the head office in Nairobi. As the largest SACCO in Africa and Kenya, Mwalimu National SACCO has a substantial workforce, with over 1,200 employees across its various branches. Approximately half of these employees—around 600 individuals—are stationed at the head office, making this location a critical hub for the SACCO's operations. The head office is where key administrative, financial, and operational activities are concentrated, making it an ideal setting for examining context awareness vulnerabilities within the BYOD environment. By focusing on this population, the study aimed to gain insights into how employees at the heart of the SACCO's operations interact with BYOD technologies and the potential security risks they face.

3.4 Sampling

Sampling is the process of selecting a subset of individuals or elements from a larger target population to participate in a study (Mcleod, 2023). This subset is used to draw conclusions or make inferences about the entire population, often when it is impractical or impossible to study the entire group (Hennink, Hutter & Bailey, 2020). In the current study, sampling involved selecting a representative group of employees from Mwalimu National SACCO's head office in Nairobi. Given that the head office has approximately 600 employees, a carefully chosen sample was used to gather data on context awareness vulnerabilities within the BYOD environment. The sample reflected the diversity of roles, experience levels, and device usage patterns within the SACCO which ensured that the findings are generalizable. The sampling strategy aimed to provide insights into the broader population while maintaining accuracy and relevance to the study's objectives.

3.4.1 Sample size calculation

Sample size calculation is the process of determining the number of observations or participants needed in a study to achieve reliable and statistically significant results (Mcleod, 2023). It ensures that the sample is large enough to accurately represent the target population while considering factors like the desired confidence level, margin of error, and variability within the population. The current study adopted, Taro Yamane formula for sample size calculation.

Therefore, applying the formula; $n = \frac{N}{1+N\,e^2}$

Where; n = sample size, N = target population, = error margin (10% or 0.1 for the current study)

Therefore; $n = \frac{600}{1+600\ (0.1^2)}$

$$n = \frac{600}{1+600\ (0.01)}$$

$n = \frac{600}{1+6} = \frac{600}{7}$ = 85.72, rounded to the nearest person, 86

Thus the sample size will be 86 participants.

TABLE 2. Population and Sample Size

Department of Work	Number of employees	Percentage	Sample Size
Finance & Strategy	117	19%	16
Marketing	98	16%	14
Records & Archives	45	8%	7
Customer Care	70	12%	10
Administration	105	17%	15
Legal	6	1%	1
Human Resources	12	2%	2
ICT	82	14%	12
Operations	65	11%	9
Total	**600**	**100%**	**86**

Source (Mwalimu National SACCO, 2024; Researcher, 2024)

3.5 Research Instrument

The study utilized a structured questionnaire as the primary research tool, designed to systematically gather data from Mwalimu SACCO employees. This questionnaire was divided into six distinct sections to ensure comprehensive coverage of all relevant aspects of the study. The first section focused on demographic details, collecting background information on respondents, including their education level, work experience, and specific roles within Mwalimu National SACCO operations. This demographic data is crucial for understanding the diverse profiles of employees and how these factors influenced their interaction with BYOD environments.

The researcher adopted structured questionnaires over interviews, due to their efficiency, consistency, and scalability in data collection. Structured questionnaires allow for standardized responses, ensuring uniform data that can be quantified and analysed statistically. In comparison, interviews are time-consuming and prone to subjective biases, instead questionnaires enable cost-effective way to reach many Mwalimu SACCO employees. Also, the Likert scale format enhances measurement precision, capturing context-aware BYOD

vulnerabilities systematically. This approach ensures reliable, comparable data, essential for developing a robust predictive model.

The subsequent five sections addressed the study's key variables. These include the independent variables for the study, notably, Access Time, Device Usage, Location, and Role Risk Factor, as well as the dependent variable, Vulnerability Score. Each section featured structured questions which were designed to measure the respective variables accurately. The questions were formulated using a Likert scale, allowing for a measured assessment of employee behaviours, device usage patterns, and potential vulnerabilities. This structured approach ensured that the data collected is both consistent and quantifiable, facilitating effective analysis. By providing clear and targeted questions, the questionnaire helped capture detailed insights into how various factors contribute to context awareness vulnerabilities in BYOD environments within SACCOs, enabling the development of a robust predictive model.

3.6 Pilot study

A pilot study was conducted to assess the viability and effectiveness of the research tool before its full deployment. The preliminary test will involve ten employees from a SACCO other than Mwalimu and Stima SACCOs, ensuring that the findings were not influenced by the primary study sample. The purpose of the pilot study was to evaluate the research tool's validity and reliability, making necessary adjustments to enhance its accuracy and consistency.

3.6.1 Validity

Validity refers to the extent to which the research tool measures what it is intended to measure. In this study, both construct validity and content validity were tested. Construct validity examined whether the questionnaire accurately captured the theoretical constructs of context awareness vulnerabilities in BYOD environments, such as access time, device usage, location and role risk factor.

Content validity was assessed by ensuring that the questionnaire comprehensively covered all relevant aspects of the study's variables, reflecting the full scope of potential vulnerabilities. Feedback from the pilot study participants was used to refine the questions, ensuring that they are clear, relevant, and effective in gathering the intended data.

3.6.2 Reliability

Reliability refers to the consistency and stability of the research tool over time. In this study, reliability was tested using Cronbach's alpha, a statistical measure that assesses the internal consistency of the questionnaire. A high Cronbach's alpha value (typically above 0.7) indicates that the questions within each section of the questionnaire are consistently measuring the same underlying concept. During the pilot study, responses from the 10 SACCO employees was analysed to determine the reliability of the tool. The reliability score is found to be satisfactory; the tool was deemed suitable for the full study.

3.7 Data Processing and Analysis

The study employed both descriptive and inferential analysis techniques in the processing and interpretation of the collected data. After participants submitted their completed questionnaires, the responses were checked for completeness and accuracy, then cleaned and prepared for entry into statistical software for coding and analysis. Descriptive analysis was used to evaluate Mwalimu SACCO employees' demographic and background information, summarizing this data through means, standard deviations, and frequency distributions. This provided a clear overview of the respondent profiles and their potential influence on BYOD practices.

3.8 Regression Analysis

For inferential analysis, the study utilized multivariate regression analysis to examine the relationship between the independent variable, which included Access Time, Device Usage, Location, and Role Risk Factor against the dependent variable, Vulnerability Score. The regression analysis operationalized the study model by identifying how each independent

variable contributes to context awareness vulnerabilities in the BYOD environment within Mwalimu National SACCO. The regression model for the study was expressed as:

$$\text{Vulnerability Score} = \beta_0 + \beta_1 (\text{Access Time}) + \beta_2 (\text{Device Usage}) + \beta_3 (\text{Location}) + \beta_4 (\text{Role Risk Factor}) + \epsilon$$

Therefore, the Equation for the model was.

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \epsilon$$

Where.

Y = Vulnerability score

β_0 = Intercept

$\beta_{1,2,3,4}$ = Beta coefficients for all the independent variables

X_1 = Access time

X_2 = Device Usage

X_3 = Location

X_4 = Role risk factor

ϵ = error term

CHAPTER FOUR

DATA ANALYSIS, FINDINGS AND DISCUSSION

4.1 Introduction

The purpose of this study is to establish a mechanism for context awareness vulnerability detection in BYOD environments using linear regression technique. To achieve this, a primary survey was carried out at Mwalimu National SACCO. SACCOs form backbone of financial institutions which have gained foothold in many Kenyan communities and continue to grow at fast rate. The study intended to find-out how, employees at a leading SACCO, faired in the scope of BYOD framework and how they understood factors for context awareness vulnerability, in effort to design a tool for context awareness detection.

4.2 Response Rate

A total of 86 questionnaires were distributed randomly to employees at Mwalimu National SACCO.

TABLE 3. Response Rate

Response	Frequency	Percentage
Responded	72	84%
Not-Responded	14	16%
Total	**86**	**100%**

The results in table 4.1, highlights the response rate for the field survey. A total of 86 questionnaires were randomly distributed to employees of Mwalimu National SACCO. A total of 72 questionnaires, representing 86% response rate were returned in time for data analysis. According to Hennink et al. (2020), a response rate of above 70% is considered excellent for data analysis as would give a good picture of the views on ground. In the current study on the detection of context awareness vulnerabilities within BYOD environment for SACCO institutions, N shall be 72.

4.3 Demographic Distribution of Respondents

The study considered four demographic data for the respondents, which included; age distribution, education level, department of work and work experience.

4.3.1 Demographic distribution by Age

In the analysis of age distribution of SACCO employees, the computation utilized frequencies and percentages.

TABLE 4. Age Distribution

Age categories	Frequency	Percent
18 - 30 years	21	29.2%
31 - 35 years	25	34.7%
36 - 40 years	18	25.0%
41 - 45 years	5	6.9%
Over 46 years	3	4.2%
Total	**72**	**100.0%**

Results on age distribution in table 4.2, show that majority of respondents 34.7% (25), and were in the age group of 31 – 35 years. Also, results show 29.2% (21) of respondents were aged between 18 – 30 years, 25.0% (18) were in age-group 36 – 40 years, 6.9% (5) were in age group 41 – 45 years. Finally, the results show that 4.2% (3) of respondents were over 46 years of age. The findings imply that, age diversity exists within the SACCO staff roster. There is also a good mixture between young staff and the old which offers a pointer to existence of good balance in staff age distribution.

4.3.2 Demographic distribution by Education Level

In the computation of age distribution of SACCO employees, the study presentation utilized frequencies and percentages.

TABLE 5. Education Level Distribution

Categories	Frequency	Percent
Certificate/Diploma	14	19.4 %
Undergraduate Degree	50	69.4 %
Post-graduate Degree	8	11.1 %
Total	**72**	**100.0 %**

Results in table 4.3, highlight respondents' education level. Majority of respondents, 69.4% (50) indicated to have undergraduate degree. Also, 19.4% (14) of the respondents indicated to have a qualification in certificate or Diploma, whereas 11.1% (8) of the respondents indicated to have attained a post-graduate Degree. These findings show that entire operational staff had attained higher education. These results imply that, academic attainment is very crucial in SACCO work force. Also, results imply educated workforce are vital in embracing operational changes such as integrating technology and more so concepts such as BYOD for work operations.

4.3.3 Demographic distribution by Department of Work

In the analysis of respondents work department at the SACCO, the computation utilized frequencies and percentages.

TABLE 6. Department of Work

Categories	Frequency	Percent
Finance & Strategy	15	20.8%
Marketing	13	18.1%
Records & Archives	4	5.6%
Customer Care	3	4.2%
Administration	15	20.8%
Human Resources	2	2.8%
ICT	11	15.3%
Operations	9	12.5%
Total	**72**	**100.0%**

Results in table 4.4, presents respondents distribution by department of work. Majority of respondents, 20.8% (15) indicated to be attached to the finance & strategy department, with an equivalent 20.8% (15) also attached to the administration department.

Further, 18.1% (13) of respondents indicated to be attached to marketing department, 15.3% (11) indicated to work in ICT division, 12.5% (9) indicated to be attached to operations department, 5.6% (4) of respondents were attached to the records & archives department, and 4.2% (3) indicated to be attached to the customer services department.

Finally, 2.8% (2) of the respondents indicated to be attached to the human resources department. Results show the sub-division of organization into different departments, which imply that to effectively deliver corporate standards of operations, it's imperative to distributed organizational activities into different department and sections.

4.3.4 Demographic distribution by Work Experience

The respondents work experience in the SACCO was analysed and computed in frequencies and percentages.

TABLE 7. Work Experience

Categories	Frequency	Percent
Below 5 years	15	20.8%
6 - 10 years	31	43.1%
11 - 15 years	17	23.6%
16 - 20 years	6	8.3%
Over 46 years	3	4.2%
Total	**72**	**100.0%**

Results in table 4.5, show distribution of respondents by work experience. Majority of respondents, 43.1% (31) indicated to have work experience of 6 – 10 years. The results also show, 23.6% (17) of the respondents have worked for 11 – 15 years, whereas 20.8% (15) have

work experience of below 5 years and 8.3% (6) of respondents indicated to have work experience of 16 – 20 years. Finally, 4.2% (3) of respondent indicated to have over 46 years of work experience.

The results highlight diversity in work experience distribution, with majority of respondents having worked for over 5 years. This implies that work experience distribution is critical to attain balance and continuity in operations across generations, with vastly experienced staff mentoring new recruits and those less experienced.

4.4 Descriptive Statistics for Context Awareness Vulnerability Factors

The first objectives of the study was to examine the factors that influence Context Awareness Vulnerability within the BYOD environment. Four factors, which include; Access time, Device usage, Location and Role risk factor were identified which formed the basis for structured survey questionnaire. The structured questionnaire was designed with a 5-point scale; where 1= strongly disagree (1 – 1.4), 2 = disagree (1.5 – 2.4), 3 = neutral meaning neither agree nor disagree (2.5 – 3.4), 4 = agree (3.5 – 4.4) and finally, 5= strongly agree (4.5 – 5). The descriptive statistics utilized means and standard deviation outputs to determine respondent's feedback as presented in the following section.

4.4.1 Descriptive statistics of access time on context awareness vulnerability in BYOD environment

The first factors examined was access time and its effect on context awareness vulnerability within BYOD environment and descriptive data computed in mean and standard deviation.

TABLE 8. Access Time Mean and Standard Deviation

Influence of access time factor on context awareness vulnerability	N	Mean	Std. Deviation
I frequently access SACCO systems after regular business hours.	72	4.74	.581
The duration of my access to SACCO data during off-hours is significant.	72	3.94	.441
I find it necessary to access SACCO systems during weekends or holidays.	72	4.71	.777
I access critical SACCO information multiple times throughout the day.	72	3.96	.262
I believe that accessing SACCO data late at night increases security risks.	72	4.56	.948
I often work on SACCO tasks that require system access outside of the office.	72	3.26	.692
My access to SACCO systems during non-peak hours is essential for my role.	72	4.82	.454
I notice an increase in system access failures or errors during after-hours access.	72	4.64	.877
The time of day impacts my ability to securely access SACCO systems.	72	4.79	.442
I believe that there should be more restrictions on after-hours access to SACCO systems.	72	3.14	.718

Results computed in table 4.6, highlight respondents' views on the influence of access time on context awareness vulnerability within BYOD environment of a SACCO. Respondents strongly agreed (mean = 4.74, standard deviation = 0.581), that they accessed SACCO systems frequently after regular business hours. Respondents agreed (Mean of 3.94 and standard deviation of 0.441) that they had significant duration of access to SACCO data during off-hours is significant. Respondents indicated that they found it necessary to access SACCO systems during weekends or holidays, with a mean of 4.71 and standard deviation of 0.777

Further, results show that respondents agreed (mean = 3.96, standard deviation = 0.262), that they had access critical SACCO information multiple times throughout the day. Also, respondents strongly agreed (mean = 4.56, standard deviation = 0.948), in the belief that accessing SACCO data late at night increases security risks. Responded were of neutral view (mean = 3.26, standard deviation = 0.692), that they worked on SACCO tasks that required system access outside of the office.

In addition, results show that respondents strongly agreed (4.82, 0.454) that their access to SACCO systems during non-peak hours is essential for their roles. Also, responded equally strongly agreed (mean = 4.64, standard deviation= 0.877) they noticed increase in system access failures or errors during after-hours access. Respondents also strongly agreed (mean = 4.79, standard deviation = 0.442) that the time of day impacts their ability to securely access SACCO systems. Finally, results show that respondents were of neutral view (mean = 3.14, standard deviation =0.718) on the need for more restrictions on after-hours access to SACCO systems.

4.4.2 Descriptive statistics of device usage on context awareness vulnerability in BYOD environment

The second factor for analysis was device usage and its effect on context awareness vulnerability within BYOD environment where data is computed in mean and standard deviation.

TABLE 9. Device Usage Mean and Standard Deviation

Influence of device usage factor on context awareness vulnerability	N	Mean	Std. Deviation
I use my personal device for work-related tasks frequently.	72	4.43	.624
My personal device has strong security measures (e.g., encryption, antivirus) in place.	72	4.25	.727
I regularly update the security features on my personal device.	72	4.10	.790
I feel comfortable using my personal device to access sensitive SACCO data.	72	4.00	.712
The applications I use on my personal device are necessary for my job.	72	4.01	.813
I occasionally share my personal device with others, even when SACCO data is accessible.	72	4.11	.779
I am aware of the potential risks of using personal devices for work.	72	4.21	.730
I believe that my personal device is more vulnerable to cyber threats than company-provided devices.	72	4.15	.685
I am careful about the types of networks I connect to when using my personal device for work.	72	3.96	.879
I believe that my device usage habits do not pose a significant risk to SACCO's data security.	72	4.10	.754

Results in table 4.7, presents respondents views on the effect of device usage on context awareness vulnerability within BYOD environment for SACCOs. Respondents agreed (mean= 4.43, standard deviation = 0.624) that they frequently utilized personal devices for work related tasks. Respondents agreed (mean = 4.25, standard deviation = 0.727) that their personal devices have strong security measures (e.g., encryption, antivirus) in place. Respondents also indicated that they updated security features of their personal devices regularly with a mean of 4.10 and standard deviation of 0.790.

Further, results show that respondents agreed (mean = 4.00, standard deviation = 0.712) that they felt comfortable using their personal devices to access sensitive SACCO data. Respondents also agreed (mean = 4.01, standard deviation = 0.813) that the applications which they used on personal devices were necessary for their job. Also, respondents agreed that they occasionally shared personal devices with others, even when SACCO data is accessible, with a mean of 4.11 and standard deviation of 0.779.

In addition, results show that respondents agreed (mean = 4.21, standard deviation = 0.730), that they were aware of the potential risks for using personal devices for work. Respondents further agreed (mean = 4.15, standard deviation = 0.685) that they believed that personal devices were more vulnerable to cyber threats than company-provided devices. Respondents also agreed that they were careful about the types of networks which they connected to when using personal device for work, with a mean of 3.96 and standard deviation of 0.879. Finally, results show that respondents agreed (mean = 4.10, standard deviation = 0.754) that their device usage habits do not pose a significant risk to SACCO's data security.

4.4.3 Descriptive statistics of location on context awareness vulnerability in BYOD environment

The third factor for examination was location and its effect on context awareness vulnerability within BYOD environment where data is computed in mean and standard deviation.

TABLE 10. Location Mean and Standard Deviation

Influence of location factor on context awareness vulnerability	N	Mean	Std. Deviation
I frequently access SACCO systems from locations outside of the office.	72	4.25	.727
I often connect to public Wi-Fi when working remotely.	72	3.99	.896
I use a VPN or other security measures when accessing SACCO systems remotely.	72	3.78	1.103
I believe that accessing SACCO data from home is as secure as from the office.	72	4.13	.855
I am concerned about the security of SACCO data when accessing it from public places.	72	4.14	.844
The location from which I access SACCO systems affects the speed and reliability of access.	72	3.92	.835
I am mindful of my surroundings when accessing SACCO systems in public.	72	4.46	.555
I prefer working from locations where I can ensure secure access to SACCO systems.	72	4.40	.725
I believe that SACCO should implement stricter controls for remote access.	72	4.31	.573
I notice a difference in the security measures required based on my access location.	72	4.00	.888

Results in table 4.8, highlight respondents feedback on the influence of location on context awareness vulnerability within BYOD environment for SACCO Institution. Respondents were in agreement (mean = 4.25, standard deviation = 0.727) that they frequently accessed SACCO systems from locations outside that office. Respondents agreed (mean = 3.99, standard deviation = 0.896), that they often connected to public Wi-Fi when working remotely.

Further, respondents agreed (mean = 3.78, standard deviation = 1.103) that they used a VPN or other security measures when accessing SACCO systems remotely. Respondents were also in agreement (mean = 4.13, standard deviation = 0.855) that accessing SACCO data from

home is as secure as from the office. Results show respondents agreed (mean = 4.14, standard deviation = 0.844), that they are concerned about the security of SACCO data when accessing it from public places. Respondents also agree that the location from which I access SACCO systems affects the speed and reliability of access, with a mean of 3.92 and standard deviation of 0.835.

In addition, results show that respondents agreed (mean = 4.46, standard deviation= 0.555) that they were mindful of their surroundings when accessing SACCO systems in public. Respondents also agreed (mean = 4.40, standard deviation = 0.725) that they preferred working from locations where they can ensure secure access to SACCO systems. Respondents indicated to agree (mean = 4.31, standard deviation = 0.573), that SACCO should implement stricter controls for remote access. Finally, results show that respondents agreed (mean = 4.00, standard deviation = 0.888) that they noticed a difference in the security measures required based on my access location.

Descriptive Statistics of Role Risk Factor on Context Awareness Vulnerability in BYOD Environment

The final factor for analysis was role risk factor and its effect on context awareness vulnerability within BYOD environment where data is computed in mean and standard deviation.

TABLE 11.Role Risk Factor Mean and Standard Deviation

Influence of role risk factor on context awareness vulnerability	N	Mean	Std. Deviation
My role within the SACCO requires frequent access to sensitive information.	72	3.86	.997
I have more access privileges than necessary to perform my job.	72	4.13	.821
My decision-making authority impacts the level of access I have to SACCO systems.	72	4.17	.856
I believe that employees in higher roles pose a greater risk to data security.	72	3.92	.835
I receive regular cyber-security training specific to my role within SACCO.	72	4.49	.503
I am confident that my role-specific access to SACCO systems is properly monitored.	72	4.35	.790
I think employees with similar roles to mine should have restricted access to certain data.	72	4.25	.687
The security protocols in place for my role are sufficient to prevent unauthorized access.	72	3.94	1.005
I believe that role-based access controls are crucial for SACCO's data security.	72	4.10	.754
I am aware of the potential risks my role poses to SACCO's cyber-security.	72	4.35	.772

The results in table 4.9, present respondents views on the influence of role risk factor on context awareness vulnerability within BYOD environment. Results show that respondents agreed (mean = 3.86, standard deviation = 0.997) that their roles within the SACCO required frequent access to sensitive information. Respondents agreed (mean = 4.13, standard deviation = 0.821) they had more access privileges than necessary to perform their jobs. Also respondents indicated to be in agreement (mean = 4.17, standard deviation = 0.856) that their decision-making authority impacts the level of access they have to SACCO systems.

Further, results show respondents agreed (mean = 3.92, standard deviation = 0.835) that employees in higher roles posed a greater risk to data security. Also, respondents agreed (mean = 4.49, standard deviation = 0.503) that they received regular cyber-security training specific to their roles within the SACCO. Respondents showed that they were in agreement that their

role-specific access to SACCO systems is properly monitored with a mean of 4.35 and standard deviation of 0.790.

In addition, results show that respondents agreed that employees should have access restrictions to certain data based on the type of their roles whose roles, with a mean of 4.25 and standard deviation of 0.687. Respondents agreed (mean = 3.94, standard deviation = 1.005), that security protocols in place for their roles are sufficient to prevent unauthorized access. Also, respondents were in agreement (mean = 4.10, standard deviation = 0.754) that role-based access controls are crucial for SACCO's data security. Finally, results show that respondents agreed (mean = 4.35, standard deviation = 0.772) that they were aware of the potential risks my role poses to SACCO's cyber-security.

4.5 Inferential Statistics

The second objective in the study was to design a regression model based on the identified factors for the detection of context awareness vulnerability within BYOD environment. Also, the third objective was to test the model and validate it. To attain these objectives, the study will perform the inferential tests, employing regression model.

4.5.1 Designing the model of the study

The factors identified in the study include; access time, device usage, location and the role risk factor. The study intends to determine whether these factors have an influence on vulnerability. The model will be conceptualized using multivariate regression model.

The basic equation for the model proposed, Y (vulnerability) $= A + \beta_n X_n + \acute{\varepsilon}$ (equation i), where, A shall be the constant of intercept between context awareness vulnerability (CAV) factors and vulnerability score (Y), β shall be the beta co-efficient for each CAV factor, X shall be the actual CAV factors, n shall be the number of vulnerability factors, and the $\acute{\varepsilon}$ shall be error margins.

Therefore, the model for the study;

$$\textit{Vulnerability Score (Y)} = \textit{Constant} + \beta_1 * \textit{Access Time} + \beta_2 * \textit{Device Usage} + \beta_3 * \textit{Location} + \beta_4 * \textit{Role Risk Factor} + \acute{\varepsilon} \quad \textit{(ii)}$$

To actualize the model, the study performed a multivariate regression equation.

4.5.2 Model testing and validation

Regression model was implemented, with independent variable, vulnerability score (Y) run against residual predictors which were dependent variables, notably; access time, device usage, location and role risk factor.

TABLE 12. Model Summary for Factors of Context Awareness Vulnerability on Vulnerability Score

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.948[a]	.899	.893	.17491

a. Predictors: (Constant), Role risk factor, Access time, Device Usage, Location

The model summary results in table 4.10, highlights the regression test outputs, where they deduced; R = 0.948 and R-Square = .899. The R output of 0.948, highlights existence of strong positive correlation between factors; access time, device usage, location and role risk factor and vulnerability score. Further, the R^2 outcome of 0.899, imply that the four factors; access time, device usage, location and role risk factor account for 89.9% of variability in context awareness vulnerability within BYOD environment, with 10.1% of variability attributed to factors which are external and not in the model.

TABLE 13. ANOVA for Factors of Context Awareness Vulnerability

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	18.161	4	4.540	148.413	.000[b]
	Residual	2.050	67	.031		
	Total	20.211	71			

a. Dependent Variable: Vulnerability Score

b. Predictors: (Constant), Role risk factor, Access time, Device Usage, Location

The Analysis of Variance (ANOVA) outputs in table 4.11, deduce; F (4, 67) = 148.413, p-value = 0.000 ($p < 0.01$). The results imply that that the study model is fit to predict context awareness vulnerability at 0.01 significant level. In addition, the study rejects null hypothesis and accepts alternative that, factors including; access time, device usage, location and role risk factor wield a significant statistical effect on context awareness vulnerability within BYOD environment and is significant at 0.01 significance level.

TABLE 14. Coefficients for Context Awareness Vulnerability

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.351	.242		5.576	.000
	Access time	.603	.061	.446	9.899	.000
	Device Usage	.793	.066	.697	12.030	.000
	Location	.772	.154	.704	11.465	.000
	Role risk factor	.698	.153	.548	9.953	.000

a. Dependent Variable: Vulnerability Score

The coefficients outputs in table 4.12 deduce; Constant (A) = 0.351, p-value of 0.000 ($p < 0.01$), beta for access time (β_1) = 0.603, p-value = 0.000 ($p < 0.01$) , beta for device usage (β_2) = 0.793, p-value = 0.000 ($p < 0.01$) , beta for location (β_3) = 0.772, p-value = 0.000 ($p < 0.01$) and beta for role risk factor (β_4) = 0.693, p-value = 0.000 ($p < 0.01$).

The model equation proposed:

$Y = A + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \acute{\varepsilon}$

Therefore, the study model deduced is:

Vulnerability Score = 0.351 + 0.603*Access Time + 0.793*Device Usage + 0.772*Location + 0.693*Role Risk Factor

The findings imply; that access time, device usage, location and role risk factor wield a positive effect on vulnerability. This is accrued for all the variables which implies that; for every single

unit change in access time results in 0.603 units change in vulnerability score, for every unit change in device usage shall result in 0.793 units change in vulnerability score, for every unit change in location results in 0.772 units change in vulnerability score and finally for every single unit change in role risk factor results in 0.693 units change in vulnerability score. The study therefore established that, factors including access time, device usage, location and role risk factor wield a strong positive effect on context awareness vulnerability within BYOD environment.

The regression results confirm that access time, device usage, location, and role risk factor significantly influence BYOD vulnerabilities, reinforcing the model's predictive strength. The positive coefficients suggest that an incremental change in these factors, vulnerability scores will rise, highlighting key security risks for SACCOs. In the case of device usage (0.793) returned the strongest effect, meaning that frequent reliance on personal devices escalates exposure to threats such as malware and data breaches. Similarly, location (0.772) indicates that accessing SACCO systems from unsecured locations increases exposure to security risks which imply a requirement for stricter location-based access controls. The influence of role risk factor (0.693) implies that higher-privilege roles face greater threats, which warrants a need for multi-factor authentication and access restrictions which are based on access-level clearance, where officials with higher level roles, should have much higher access-security clearance. These findings enable SACCOs to implement targeted cyber-security measures, such as access time policies, secure authentication mechanisms, and real-time monitoring, necessary in limiting and reducing context-aware BYOD vulnerabilities. The model's strong predictive power makes it a valuable tool for proactive risk management in financial institutions.

4.6 Discussion of Findings

The main objective of this study is to determine context awareness vulnerability detection in BYOD environment using regression model. Four factors including access time, device usage, location and role risk factor were examined in regard to their effect on vulnerability. The study established that access time wielded significant effect on vulnerability score. Findings show that any incremental change in access time, results in an incremental change in context awareness vulnerability. These findings are supported in conclusions by Annansingh (2020) who noted that convenience and access time were primary drivers for professionals to integrated personal devices in work related activities. The findings show that, more access to personal devices, increased exposure to cyber-security vulnerabilities thus highlighting the importance of awareness of underlying threats while accessing personal devices for work purposes.

The study also established that device usage wields a positive effect on context awareness vulnerability within BYOD environment. Any incremental changes in device usage significantly increases context awareness vulnerability. The findings support previous conclusions in studies by Sikder et al. (2021) and, Kreeft and Govender (2022) who identified the increased exposure to cyber-security vulnerabilities, as a result of increased device usage in work operations or business activities. In addition, the findings showed the importance of cyber-security awareness in device usage, which is consistent with Adeyelure, and Segooa (2024) findings on importance of cyber security training to enhance awareness in usage of personal devices for work activities.

Further, the study established that location wielded in impact on vulnerability. An incremental change in location accrues a spike in incremental change in context awareness vulnerability. These findings are consistent with conclusions of Maseko's (2023), who noted that frequent deviation from security protocol in usage of personal devices in different places

contributed to increasing the exposure to cyber security risks. The findings are also in line with submissions of Kholoanyane's (2020) who noted that usage of devices continuously change and in different locations increases the level of risks associated with exposures to cyber-security vulnerability. Both Maseko's (2023) and Kholoanyane's (2020) were consistent on importance of importance of continuously employing cyber security protocols whenever utilizing personal devices for work, which requires training and constant awareness of locations where personal devices are used.

In addition, the study established that role risk factor had an effect in vulnerability score. Any incremental change in role risk factor, contributed to an increased level of context awareness vulnerability. These findings are supported in conclusions by Muthuswamy (2023), who opined that digital workspaces and employee roles in utilizing different devices were hugely influenced by the kind of work they undertook. The findings show that, with increased level of operational responsibility, the level of risks to cyber-security increased thus need for constant levels of cyber- security risks which is engrained in training. Also, findings are in line with Ferdousi (2022) who concluded that strictness in enforcing BYOD policies across all roles within an organization was critical in putting reliable defence against potential cyber security threats that an organization may face across different organization sections and positions.

The regression results confirm that access time, device usage, location, and role risk factor significantly influence BYOD vulnerabilities, reinforcing the model’s predictive strength. The positive coefficients suggest that an incremental change in these factors, vulnerability scores will rise, highlighting key security risks for SACCOs. In the case of device usage (0.793) returned the strongest effect, meaning that frequent reliance on personal devices escalates exposure to threats such as malware and data breaches. Similarly, location (0.772) indicates that accessing SACCO systems from unsecured locations increases exposure to security risks which imply a requirement for stricter location-based access controls. The

influence of role risk factor (0.693) implies that higher-privilege roles face greater threats, which warrants a need for multi-factor authentication and access restrictions which are based on access-level clearance, where officials with higher level roles, should have much higher access-security clearance. These findings enable SACCOs to implement targeted cyber-security measures, such as access time policies, secure authentication mechanisms, and real-time monitoring, necessary in limiting and reducing context-aware BYOD vulnerabilities. The model's strong predictive power makes it a valuable tool for proactive risk management in financial institutions.

4.7 Summary

This section of the study covered the analysis and presentation of data collected on context awareness vulnerability detection within BYOD environment using regression model. The section covered demographic section which contained respondents background information, descriptive statistics section which covered factors for context awareness vulnerability notably; access time, device usage, location and role risk factor. The section further examined the inferential statistics where the study proposed and model which was actualized with a multivariate regression equation and finally discussed the findings.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This section covers summary, conclusion and discussion of contribution of the current study which focused on context awareness vulnerability detection in BYOD environments utilizing multivariate regression analysis model.

5.2 Summary of the Findings

5.2.1 Access time and context awareness vulnerability

One of the key findings of the study is that access time significantly affects context awareness vulnerability. Respondents frequently accessed SACCO systems after business hours and during weekends or holidays. This off-hours access was seen as critical for fulfilling their roles, but it also heightened the security risks. Participants strongly agreed that accessing SACCO data late at night posed greater security risks, particularly because of the increased system failures and errors experienced during this time. Despite recognizing these risks, respondents were neutral on whether more restrictions should be imposed on after-hours access. This suggests that while after-hours access is crucial for operational efficiency, it also opens avenues for security vulnerabilities, highlighting the need for stronger after-hours security protocols.

5.2.2 Device usage and vulnerability

The study found that device usage has a significant impact on context awareness vulnerability. Respondents frequently used their personal devices for work-related tasks and believed that their devices had adequate security measures such as encryption and antivirus software. However, despite regular updates and security measures, respondents acknowledged the inherent risks associated with using personal devices for work. They expressed comfort in accessing sensitive SACCO data from their devices but recognized that personal devices might be more vulnerable to cyber threats than company-provided devices. The sharing of personal

devices, even when SACCO data was accessible, further exacerbated the risk. The study also noted that while respondents were cautious about connecting to secure networks, device usage still posed a significant threat to data security due to these inherent vulnerabilities.

5.2.3 Location and vulnerability

Location was another critical factor in determining context awareness vulnerability. Employees often accessed SACCO systems from various locations outside the office, including public places. Despite this, many respondents were comfortable with remote access, provided they employed additional security measures such as virtual private networks (VPNs). However, there was concern about the security of SACCO data when accessed from public locations, where the use of unsecured public Wi-Fi networks increased the vulnerability to cyber threats. The study showed that location influences the speed and reliability of system access and that respondents preferred working in locations where secure access could be ensured. Furthermore, there was a call for stricter controls on remote access to safeguard SACCO data. Although respondents were mindful of their surroundings in public spaces, the differences in security measures based on access location remained a notable vulnerability factor.

5.2.4 Role risk factor and vulnerability

The role risk factor was another important determinant of vulnerability in BYOD environments. Employees in higher roles, with access to sensitive information and decision-making authority, were identified as posing a greater risk to data security. Respondents felt that their roles required more access privileges than necessary, which could lead to heightened vulnerability. However, most respondents reported receiving regular cyber-security training specific to their roles, which helped mitigate some of the risks associated with their positions. The study highlighted the importance of monitoring role-specific access and enforcing role-based access controls to maintain SACCO's data security. The findings also emphasized the

need for employees to be aware of the potential risks posed by their roles and the significance of restricting access to sensitive data based on job functions.

5.3 Conclusions

The current study was guided by three objectives, notably; to investigate factors that influence vulnerabilities in BYOD environment, to design and develop a regression model for BYOD using the identified factors and to test and validate the model. The study makes the following conclusions based on the objectives.

5.3.1 Factors influencing vulnerabilities in BYOD environments

This study identified four key factors, which included access time, device usage, location, and role risk factor, that significantly wield an influence on context awareness vulnerabilities in BYOD environments. Study concludes that access time is a critical vulnerability driver, particularly during non-standard hours such as nights, weekends, and holidays. For employees who access systems during these times face heightened risks due to increased system access failures, reduced oversight, and relaxed security protocols. In addition, device usage was identified as another significant factor, with vulnerabilities linked to personal device security measures, such as inadequate encryption, infrequent updates, and sharing devices with others. These habits expose sensitive SACCO data to potential threats.

Location aspect was found to contribute significantly to vulnerabilities. Employees accessing systems from public spaces, using unsecured Wi-Fi, or bypassing VPNs were found to face greater risks compared to secure office environments. Lastly, the study concludes that role risk factor highlighted the influence of organizational roles on vulnerabilities. Employees who have high-level responsibilities and broader system access privileges face greater risks, especially when role-based access controls and security protocols are insufficient.

5.3.2 Design and development of a regression model

The study successfully designed and implemented a multivariate regression model to establish the relationship between the identified factors and vulnerability levels. The model demonstrated a strong positive correlation between access time, device usage, location, and role risk factor and the overall context awareness vulnerability. The Statistical results show that these factors combined account for 89.9% of the variability in vulnerability, highlighting the model's robustness. This predictive framework is useful for organizations like SACCOs, to enabling them monitor and mitigate risks in their BYOD environments systematically. Through quantifying the impact of each factor, the model provides actionable steps for formulating a tailored security measures and prioritizing areas with the highest vulnerability potential.

5.3.3 Testing and validation of the model

The multivariate regression model was tested and validated through inferential statistical techniques. The results noting outputs from ANOVA and coefficient analysis confirmed the model's ability to predict vulnerabilities with high accuracy, with all factors showing significant effects at the 0.01 significance level. These findings validated the model's reliability as a tool for detecting vulnerabilities, offering organizations a mechanism to assess and manage risks effectively. The study rejected the null hypothesis, therefore confirming that access time, device usage, location, and role risk factor are critical contributors to context awareness vulnerabilities, reinforcing the need for targeted cyber-security policies and regular employee training.

5.3.4 Deployment of linear regression based vulnerability detection model in SACCOs

The study proposes the following roadmap for the successfully implementation of regression-based context awareness vulnerability detection model in SACCOs;

The first step involves assessing the existing cyber-security infrastructure to identify vulnerabilities associated with BYOD usage. A comprehensive cyber-security audit should be

conducted to evaluate current risk levels, assess network security, and determine the extent of employee device access. SACCOs must also ensure that secure network access, endpoint protection tools, and real-time monitoring systems are in place before integrating the model. Following the assessment, the next step shall be the development and integration of the multivariate regression model within the SACCO's security framework. This involves configuring the model to track key risk factors such as access time, device usage, location, and role risk factors. For integration of the model with existing IT security systems, SACCOs can generate automated risk scores that enable real-time vulnerability detection, ensuring proactive threat mitigation.

Upon integration of the model, it is crucial to establish and enforce BYOD security policies tailored to SACCO operations. The main aspects of cyber-security policy should include the implementation of multi-factor authentication (MFA), role-based access control (RBAC), and network segmentation to restrict unauthorized access. Employees accessing SACCO systems through use of personal devices should have predefined security clearance levels based on their risk profiles, ensuring that high-risk access is adequately managed. Alongside policy enforcement, employee awareness and training programs must be introduced to enhance cyber-security consciousness. Employees should be trained on BYOD risks, secure device usage, and the importance of frequent security updates. Execution of regular security drills, such as simulated phishing attacks and vulnerability testing, can further reinforce awareness and ensure compliance with security protocols.

Continuous monitoring and improvement of the model are necessary to ensure its effectiveness. Real-time alerts and periodic security assessments should be deployed to track evolving threats, with SACCOs regularly updating the model through in-putting current data trends. A cyber-security incident response team should be set-up with objective of addressing emerging threats promptly and mitigate potential security breaches. Additionally, evaluation

and scaling are key to optimizing the model's deployment. Pilot testing should be conducted in a controlled SACCO environment before full implementation, allowing for necessary refinements based on initial results. Post-implementation, an analysis of vulnerability trends will help determine the model's effectiveness, ensuring that security measures are adapted to emerging BYOD risks. Scaling the model to other SACCO branches will further strengthen cyber-security measures across the organization, which underscores resilience in the face of cyber threats while maintaining operational efficiency. By adopting this structured approach, SACCOs can effectively balance BYOD flexibility with robust security measures, which boosts their capacity to predict, monitor, and mitigate cyber-security risks within the digital workspace.

5.4 Contributions of the Study

This study contributes to the growing body of knowledge on cyber-security in Bring Your Own Device (BYOD) environments, focusing on the detection of context awareness vulnerabilities through a regression-based approach. The study provides practical and theoretical insights that are crucial for organizations, particularly SACCOs, aiming to enhance cyber-security measures in light of the increasing adoption of BYOD frameworks.

One of the most significant contributions of this study is the development of a multivariate regression model that can predict context awareness vulnerabilities based on key factors: access time, device usage, location, and role risk factor. This model not only provides a quantitative understanding of how these factors contribute to vulnerability but also offers a mechanism for organizations to predict the likelihood of cyber-security risks under specific conditions. By integrating these factors into a model, organizations can make data-driven decisions on where to focus their cyber-security efforts and how to minimize exposure to vulnerabilities.

This contribution is particularly valuable for SACCOs and other financial institutions, where data security is of paramount importance. The model equips these organizations with a tool for early detection of potential vulnerabilities, enabling them to implement preventive measures before cyber threats escalate into significant security breaches.

The study offers practical insights into the ways organizations can improve their security protocols in BYOD environments. First, the findings highlight the need for enhanced security measures during off-hours access, a common practice in BYOD settings. Since employees frequently access sensitive organizational data outside regular business hours, the study suggests that organizations implement stricter security protocols during these times, such as multi-factor authentication and increased monitoring of system usage.

Secondly, the study underscores the importance of training and awareness regarding personal device usage. Although employees believe their personal devices are secure, the study reveals that these devices are more vulnerable to cyber threats compared to company-provided ones. By providing recommendations for better management of personal devices such as frequent security updates and using secure networks the study contributes to strengthening organizational defenses against potential breaches originating from employee devices.

On a theoretical level, this study adds to existing research on cyber-security in BYOD environments by demonstrating the interplay between access time, device usage, location, and role risk factor in shaping an organization's vulnerability landscape. These factors have often been studied in isolation, but this study integrates them into a comprehensive model, offering a holistic view of their combined effects on cyber-security.

In employing this approach, the study advances theoretical frameworks that inform future research on cyber-security vulnerabilities in BYOD settings. Researchers can build on this model to explore additional variables, refine existing ones, or apply it to other organizational contexts beyond SACCOs. The focus on SACCOs, an area that has seen

relatively limited cyber-security research, also opens up avenues for more industry-specific studies that address the unique challenges faced by financial institutions in adopting BYOD frameworks.

The study provides specific recommendations for SACCOs regarding the adoption and implementation of cyber-security policies tailored to the BYOD environment. Given the positive correlation between context awareness vulnerabilities and factors like access time and device usage, SACCOs can take action by introducing stricter access controls, enforcing role-based privileges, and monitoring employee access based on location.

Through alignment of organizational policies with these findings, SACCOs can mitigate risks while still allowing employees the flexibility to work from personal devices and remote locations. This contribution is crucial for SACCOs seeking to balance operational efficiency with robust cyber-security protocols in the increasingly digital workspace.

5.4.1 Original contribution of the study

The current study makes a unique contribution to the field of cyber-security, particularly in the context of BYOD environments within SACCOs. The primary contribution is the development of a multivariate regression model tailored to predict context awareness vulnerabilities based on critical factors notably; access time, device usage, location, and role risk factor. Existing cyber-security models, focus on generalized risk assessment, whereas this study provides a targeted, data-driven approach that quantifies the relationship between these factors and cyber-security vulnerabilities. The study also provides new insights that are specific to SACCOs, an area that has received limited cyber-security research, by identifying sector-specific risks and recommending actionable security measures tailored to financial cooperatives.

In theoretical relevance, the current study enhances existing cyber-security frameworks by integrating multiple context related factors into a single predictive model. In view of prior research and past studies, most of these factors were observed in isolation, whereas in this study

demonstrates their combined effect, which presents a more general view of vulnerability dynamics. This approach advances theoretical understandings of context awareness in BYOD environments, laying the groundwork for future research in this domain.

The adoption and application of regression-based model is a key methodological contribution, which enables organizations to predict and quantify cyber-security risks based on historical data. Regression analysis is valuable for identifying relationships between variables, providing an interpretable model that SACCOs can utilize in making proactive cyber-security decisions. However, while regression is effective in establishing statistical correlations, it may not be the best model for detecting real-time threats, as it assumes linear relationships and may struggle with non-linear cyber-security patterns. Alternative models in machine learning techniques notably; decision trees, neural networks, or anomaly detection algorithms, wield capacity to enhance predictive accuracy by capturing complex, evolving cyber threats. However in strategic cyber-security planning, the regression-based approach offer robust tool for understanding and mitigating vulnerabilities in SACCO BYOD environments.

5.5 Recommendations for Future Research

Based on results of this study, several areas for future research have emerged, particularly in the context of cyber-security in BYOD environments. First, while this study focused on specific factors such as access time, device usage, location, and role risk factor, future research could explore additional variables that may influence context awareness vulnerabilities. These could include factors like employee behaviour, organizational culture, or the specific nature of the work being performed in BYOD settings. Investigating these dimensions could provide a more comprehensive understanding of the risk landscape.

Second, future research could examine the effectiveness of different cyber-security measures or interventions in mitigating BYOD-related vulnerabilities. For instance, studies could evaluate the impact of advanced security technologies such as zero-trust architecture,

machine learning-based intrusion detection systems, or biometric authentication on BYOD security.

Third, there is scope for cross-industry comparative studies that assess BYOD vulnerabilities in different sectors beyond SACCOs, such as healthcare, education, and government institutions. This would provide insights into sector-specific challenges and solutions, broadening the applicability of the findings.

REFERENCES

Abdullah, S., & Bakar, K. A. A. (2018). Towards Secure Risk-Adaptable Access Control in Cloud Computing. *International Journal of Advanced Computer Science and Applications*, *9*(12).

Aguboshim, F. C., Udobi, J. I., & Otuu, O. O.(2023) Security Issues Associated with Bring Your Own Device (BYOD): A Narrative. *Research Highlights in Science and Technology, 2*, 167 - 186.

Ahmad, Z., Ong, T. S., Gan, Y. W., Liew, T. H., & Norhashim, M. (2022). Predictors of employees' mobile security practice: an analysis of personal and work-related variables. *Applied Sciences*, *12*(9), 4198.

Aldawood, H., & Skinner, G. (2019, May). Challenges of implementing training and awareness programs targeting cyber security social engineering. In *2019 cyber-security and cyber-forensics conference (ccc)* (pp. 111-117). IEEE.

Almarhabi, K. A., Alghamdi, A. M., & Bahaddad, A. A. (2022). Adoption of the Bring Your Own Device (BYOD) Approach in the Health Sector in Saudi Arabia. *IJCSNS Int. J. Comput. Sci. Netw. Secur*, *6*, 371-382.

Al-Mohannadi, H. (2019). *Cyber Attack Modelling using Threat Intelligence. An investigation into the use of threat intelligence to model cyber-attacks based on elasticsearch and honeypot data analysis* (Doctoral dissertation, University of Bradford).

Alushula, P. (2023, September, 7). Insider fraud bleeds SACCOs Sh118 million in past 2 years. Available online: https://www.businessdailyafrica.com/bd/economy/insider-fraud-bleeds-saccos-sh118-million-in-past-2-years--4361892 (Accessed on 24th October 2024).

Annansingh, F. (2020). Bring your own device to work: how serious is the risk?. *Journal of Business Strategy*, *42*(6), 392-398.

Asikhia, A., Osinowo, O., & Kassim, S. K. (2021). Integrating just in time theory, resource based view theory, and rational choice theory in enhancing managements' efficiency. *South Asian Research Journal of Business and Management*, *3*(1), 14-22.

Atlam, H. F., Azad, M. A., Alassafi, M. O., Alshdadi, A. A., & Alenezi, A. (2020). Risk-based access control model: A systematic literature review. *Future Internet*, *12*(6), 103.

Augusto, J. C. (2022). Contexts and context-awareness revisited from an intelligent environments perspective. *Applied Artificial Intelligence*, *36*(1), 2008644.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*.

Balega, M., Farag, W., Wu, X. W., Ezekiel, S., & Good, Z. (2024). Enhancing IoT Security: Optimizing Anomaly Detection through Machine Learning. *Electronics*, *13*(11), 2148.

Bernhardt, A., Kresge, L., & Suleiman, R. (2023). The data-driven workplace and the case for worker technology rights. *ILR Review*, *76*(1), 3-29.

Blossfeld, H. P., & Prein, G. (2019). The Relationship between Rational Choice Theory and Large-scale Data Analysis—Past Developments and Future Perspectives. In *Rational choice theory and large-scale data analysis* (pp. 3-27). Routledge.

Bradbury, K., Doe, S., & Palmquist, M. (2022). Networking across the curriculum: challenges, contradictions, and changes. *COMPOSITION ADMINISTRATION*, 203.

Ciuri, S. (2023, April, 30).Former officials of Metropolitan Sacco to face court over loss of Sh7bn. Available Online: https://nation.africa/kenya/business/former-

officials-of-metropolitan-sacco-to-face-court-over-loss-of-sh7bn-4217760 (Accessed on 14th August 2024).

Chigada, J., & Daniels, N. (2021). Exploring information systems security implications posed by BYOD for a financial services firm. *Business Information Review*, *38*(3), 115-126.

Chizoba, O. J., & Kyari, B. A. (2020). Ensemble classifiers for detection of advanced persistent threats. *Global Journal of Engineering and Technology Advances*, *2*(2), 001-010.

Churakova, Y., & Novikov, O. (2023). *A method of detecting and predicting attack vectors based on genetic programming*. (Master's Disseratation, Blekinge Institute of Technology).

Dalla, G. M. (2021). *A Model Of Byod Integration To Increase Corporate Information Security In Banks: Case Of Equity Bank Kenya*. (Masters dissertation, KCA University).

Danish, M. (2024). Enhancing Cyber Security through Predictive Analytics: Real-Time Threat Detection and Response. *arXiv preprint arXiv:2407.10864*.

Downer, K., & Bhattacharya, M. (2022, February). BYOD security: A study of human dimensions. In *Informatics* (Vol. 9, No. 1, p. 16). MDPI.

Dzuya, W. (2023, September). 12 employees linked to Ksh.160M fraud at NIS Sacco face 232 charges. Available online: https://www.citizen.digital/news/12-employees-linked-to-ksh160m-fraud-at-nis-sacco-face-232-charges-n328126 (Accessed on 15th August 2022).

Espinha Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2020). Sifu-a cybersecurity awareness platform with challenge assessment and intelligent coach. *Cybersecurity*, *3*(1), 24.

Ferdousi, B. (2022). Cyber security risks of bring your own device (BYOD) practice in workplace and strategies to address the risks. *International Journal of Science Academic Research*, *3*(10), 4554-4558.

Fernandez-Rojas, R., Perry, A., Singh, H., Campbell, B., Elsayed, S., Hunjet, R., & Abbass, H. A. (2019). Contextual awareness in human-advanced-vehicle systems: a survey. *IEEE Access*, *7*, 33304-33328.

Ganiyu, S. O., & Jimoh, R. G. (2021). Extended risk-based context-aware model for dynamic access control in bring your own device strategy. *Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics: Theories and Applications*, 295-315.

Grassett, S. (2022). *Enhanced Organizational Security Awareness: A Qualitative Study*. Capitol Technology University.

Guner, H., & Acarturk, C. (2020). The use and acceptance of ICT by senior citizens: a comparison of technology acceptance model (TAM) for elderly and young adults. *Universal Access in the Information Society*, *19*(2), 311-330.

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative research methods*. Sage.

Hudik, M. (2019). Two interpretations of the rational choice theory and the relevance of behavioral critique. *Rationality and Society*, *31*(4), 464-489.

Jamal, F., Taufik, M., Abdullah, A. A., & Hanapi, Z. M. (2020). A systematic review of bring your own device (BYOD) authentication technique. *In Journal of Physics: Conference Series*, *1529* (4), 042071. IOP Publishing.

Jimshith, V. T. (2024). An Evaluation of the Proposed Security Access Control for BYOD Devices with Mobile Device Management (MDM). *International Journal of Electrical and Electronics Research*, *12*(1), 276-285.

Kaluarachchi, P. K. (2017). *Cyber-security: stochastic analysis and modelling of vulnerabilities to determine the network security and attackers behaviour*. (Doctoral Dissertation, University of South Florida)

Kariuki, J. (2018, 13th November). *Three hackers held in SACCOs fraud crackdown*. Available Online: https://www.businessdailyafrica.com/bd/corporate/companies/three-hackers-held-in-saccos-fraud-crackdown-2227466 (Accessed on 23rd October 2024).

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, *12*(10), 417.

Khambhammettu, H., Boulares, S., Adi, K., & Logrippo, L. (2013). A framework for risk assessment in access control systems. *Computers & Security*, *39*, 86-103.

Kholoanyane, M. E. (2020*). Security awareness and training policy guidelines to minimize the risks of BYOD in a South African SME*. (Doctoral Dissertation, Northwest University).

Klein, G., & Zwilling, M. (2024). The weakest link: employee cyber-defense behaviours while working from home. *Journal of Computer Information Systems*, *64*(3), 408-422.

Kreeft, C., & Govender, K. K. (2022). Information Technology Risks Associated With Employee Non-Compliance With The Organizational "Bring-Your-Own-Device" Policy. *Journal of Positive School Psychology*, *6*(10), 2448-2459.

Lepoutre, J., & Oguntoye, A. (2018). The (non-) emergence of mobile money systems in Sub-Saharan Africa: A comparative multilevel perspective of Kenya and Nigeria. *Technological Forecasting and Social Change*, *131*, 262-275.

Lopes, S. S., Lousã, M. D., & Almeida, F. (2023). The Risks Associated With ITIL Information Security Management in Micro Companies. In *Fraud Prevention, Confidentiality, and Data Security for Modern Businesses* (pp. 1-36). IGI Global.

Maina, P. K. (2023). *Effect of Innovation Strategies on Competitive Advantage of Mwalimu National Sacco in Nairobi* (Doctoral dissertation, University of Nairobi).

Malatji, W. R., Eck, R. V., & Zuva, T. (2020). Understanding the usage, modifications, limitations and criticisms of technology acceptance model (TAM). *Advances in Science, Technology and Engineering Systems Journal*, *5*(6), 113-117.

Maseko, A. E. (2023). *Remedies to reduce user susceptibility to phishing attacks* (Doctoral dissertation, University of the Western Cape).

Mawla, T., Gupta, M., & Sandhu, R. (2022, June). BlueSky: Activity Control: A Vision for" Active" Security Models for Smart Collaborative Systems. In *Proceedings of the 27th ACM on symposium on access control models and technologies* (pp. 207-216).

Mbugua, A. N. (2020). *Impact Of Forensic Accounting Practices On Fraud Detection And Prevention Among Deposit Taking Saccos In Nairobi County* (Doctoral dissertation, University of Nairobi).

Mcleod, S. (2023). Qualitative vs quantitative research methods & data analysis. *simplypsychology. Org.*

Mironenko, I. A. (2020). Boris Ananiev's theory of self-determination of human development. In *Oxford Research Encyclopedia of Psychology*.

Moeketsi, C. B., Adeyelure, T. S., & Segooa, M. A. (2024). An Information Security Assessment Model for Bring Your Own Device in the South African Healthcare Sector. *International Journal of Science Annals, 7*(2), 2024.

Mphahlele, T. (2024). *Developing a cyber-security framework for commercial banks in South Africa.* (Doctoral Dissertation, University of Cape Town).

Munuo, J. (2024). *Protecting Personal Identifiable Information in the Financial Services Sector With Zero Trust Architecture* (Doctoral dissertation, The George Washington University).

Muthuswamy, V. V. (2023). Cyber Security Challenges Faced by Employees in the Digital Workplace of Saudi Arabia's Digital Nature Organization. *International Journal of Cyber Criminology*, *17*(1), 40-53.

Mwendwa, K. M. (2021). *A Honeypot based malware analysis tool for SACCOs in Kenya* (Doctoral dissertation, Strathmore University).

Natasia, S. R., Wiranti, Y. T., & Parastika, A. (2022). Acceptance analysis of NUADU as e-learning platform using the Technology Acceptance Model (TAM) approach. *Procedia Computer Science, 197*, 512-520.

Noor, Z., Hina, S., Hayat, F., & Shah, G. A. (2023). An intelligent context-aware threat detection and response model for smart cyber-physical systems. *Internet of Things, 23*, 100843.

Ofusori, L. O. (2019). *Three-dimensional security framework for BYOD enabled banking institutions in Nigeria* (Doctoral dissertation).

Opoku, M. O., & Enu-Kwesi, F. (2019). Relevance of the technology acceptance model (TAM) in information management research: A review of selected empirical evidence. *Research journal of business and management*, *7*(1), 34-44.

Ostrom, E. (2019). Institutional rational choice: An assessment of the institutional analysis and development framework. In *Theories of the Policy Process, Second Edition* (pp. 21-64). Routledge.

Osuagwu, L. (2020). Research methods: Issues and research direction. *Business and Management Research*, *9*(3), 46-55.

Ozer, M., Kose, Y., Bastug, M., Kucukkaya, G., & Varlioglu, E. R. (2024). The Shifting Landscape of Cybersecurity: The Impact of Remote Work and COVID-19 on Data Breach Trends. *arXiv preprint arXiv:2402.06650*.

Palanisamy, R., Norman, A. A., & Mat Kiah, M. L. (2022). BYOD policy compliance: Risks and strategies in organizations. *Journal of Computer Information Systems, 62*(1), 61-72.

Rah, A. (2023). *Device Management in the Security of "Bring Your Own Device"(BYOD) for the Post-pandemic, Remote Workplace*. (Doctorate Dissertation, University of Fairfax).

Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*(1), 24-46.

Sallis, J. E., Gripsrud, G., Olsson, U. H., & Silkoset, R. (2021). *Research methods and data analysis for business decisions*. Springer International Publishing.

SACCO Societies Regulatory Authority [SASRA] (2022). *SACCO Supervision Annual Report, 2022*. Available online : https://www.sasra.go.ke/download/sacco-supervision-annual-report-2022/ ; (Accessed on 14th August 2024).

Shah, N., & Shankarappa, A. (2018, October). Intelligent risk management framework for BYOD. In *2018 IEEE 15th International Conference on e-Business Engineering (ICEBE)* (pp. 289-293). IEEE.

Shukry, A. I. M., Rosman, M. R. M., Rosli, N. N. I. N., Alias, N. R., Razlan, N. M., & Alimin, N. A. (2023). Bring-Your-Own-Device (BYOD) and Productivity: Instrument Development and Validation. *International Journal of Interactive Mobile Technologies*, *17*(11).

Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. S. (2021). A survey on sensor-based threats and attacks to smart devices and applications. *IEEE Communications Surveys & Tutorials*, *23*(2), 1125-1159.

Sirma, J., Abeka, S. O., & Okelo, B. (2019). Assessing the Current Status of Information Security Policies among SACCOs in Kenya.

Tambasi, J. R. (2019). *Influence Of Electronic Delivery Services On Customer Satisfaction In Savings And Credit Cooperatives, A Case Of Mwalimu National Sacco, Kenya* (Doctoral dissertation, University of Nairobi).

Taylor, M., Klein, E. J., Munakata, M., Trabona, K., Rahman, Z., & McManus, J. (2019). Professional development for teacher leaders: Using activity theory to understand the complexities of sustainable change. *International Journal of Leadership in Education*, *22*(6), 685-705.

Ussatova, O., Karyukin, V., Zhumabekova, A., Begimbayeva, Y., & Ussatov, N. (2023, December). Designing a vulnerability threat detection scanner with the use of machine learning models. In *Proceedings of the 13th International Conference on Advances in Information Technology* (pp. 1-8).

Veljkovic, I., & Budree, A. (2019). Development of Bring-Your-Own-Device Risk Management Model: A Case Study From a South African Organisation. *Electronic Journal of Information Systems Evaluation*, *22*(1), 1-14.

Wangu, M. C. (2021). *Fraud risk management techniques and financial performance: the case of Savings and Credit Cooperative Organizations in Kenya* (Doctoral dissertation, Strathmore University).

Wani, T. A., Mendoza, A., Gray, K., & Smolenaers, F. (2022). Status of bring-your-own-device (BYOD) security practices in Australian hospitals–a national survey. *Health Policy and Technology*, *11*(3), 100627.

Wanjala, K., & Riitho, D. G. (2020). Internal control systems implementation and fraud mitigation nexus among deposit taking Saccos in Kenya. *Finance & Economics Review*, *2*(1), 11-29.

Yasnitsky, A. (2019). *Questioning Vygotsky's legacy*. New York: Routledge.

Zambrano, F. R. R., & Rafael, G. D. R. (2018). Bring your own device: a survey of threats and security management models. *International Journal of Electronic Business*, *14*(2), 146-170.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behaviour: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97.

APPENDICES

APPENDIX I: INTRODUCTION LETTER

Jeremiah Njoroge

KCA University

P.O Box 56808 – 00200,

Kiambu Road, Nairobi City.

Date: 12th September 2024

Dear Respondent,

I hope this message finds you well. I am a graduate student at KCA University, currently pursuing a Master of Science degree in Information Systems Management. As part of the requirements for completing my degree, I am conducting research titled, "Context Awareness Vulnerabilities Detection in BYOD Environments Using a Linear Regression Technique."

The purpose of this research is to investigate potential vulnerabilities in Bring Your Own Device (BYOD) environments and develop a predictive model to enhance security protocols. Your participation in this study is vital, as it will help provide critical insights into context-aware security practices.

Please be assured that your participation is voluntary, and all responses will be treated with complete confidentiality and anonymity. No personally identifiable information will be disclosed, and the data collected will be used solely for academic purposes.

I would greatly appreciate your involvement and support in this research endeavour. Should you have any questions, please feel free to contact me directly.

Thank you for your time and consideration.

Sincerely,

Jeremiah Njoroge

Master of Science in Information Systems Management – Class of 2024

APPENDIX II: QUESTIONNAIRE

SECTION A: BACKGROUND INFORMATION

1. Age Distribution

i. 18 – 30 years ☐
ii. 31 – 35 years ☐
iii. 36 – 40 years ☐
iv. 41 – 45 years ☐
v. Over 46 years ☐

2. Education Level

i. O-level Education ☐
ii. Certificate/Diploma ☐
iii. Undergraduate Degree ☐
iv. Post- Graduate Degree ☐

3. Department of Work

i. Finance & Strategy ☐
ii. Marketing ☐
iii. Records & Archives ☐
iv. Customer Care ☐
v. Administration ☐
vi. Legal ☐
vii. Human Resources ☐
viii. ICT ☐
ix. Operations ☐

4. Work Eperience

i. Below 5 years ☐
ii. 6 – 10 years ☐
iii. 11 – 15 years ☐
iv. 16 – 20 years ☐
v. Over 20 years ☐

In the subsequent sections, kindly indicate how much you agree/disagree with the following statements on a scale of 1 to 5 as per the table below:

Level of Agreement				
(1)	(2)	(3)	(4)	(5)
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

SECTION B: ACCESS TIME

Please indicate the extent to which you agree with the following statement on Access time on context awareness vulnerabilities in BYOD Environment.

No.	STATEMENTS	RATING				
		(1)	(2)	(3)	(4)	(5)
1.	I frequently access SACCO systems after regular business hours.					
2.	The duration of my access to SACCO data during off-hours is significant.					
3.	I find it necessary to access SACCO systems during weekends or holidays.					
4.	I access critical SACCO information multiple times throughout the day.					
5.	I believe that accessing SACCO data late at night increases security risks.					
6.	I often work on SACCO tasks that require system access outside of the office.					
7.	My access to SACCO systems during non-peak hours is essential for my role.					
8.	I notice an increase in system access failures or errors during after-hours access.					
9.	The time of day impacts my ability to securely access SACCO systems.					
10.	I believe that there should be more restrictions on after-hours access to SACCO systems.					

SECTION C: DEVICE USAGE						
Please indicate the extent to which you agree with the following statement on Device usage on context awareness vulnerabilities in BYOD Environment.						
No.	**STATEMENTS**	**RATING**				
		(1)	**(2)**	**(3)**	**(4)**	**(5)**
1.	I use my personal device for work-related tasks frequently.					
2.	My personal device has strong security measures (e.g., encryption, antivirus) in place.					
3.	I regularly update the security features on my personal device.					
4.	I feel comfortable using my personal device to access sensitive SACCO data.					
5.	The applications I use on my personal device are necessary for my job.					
6.	I occasionally share my personal device with others, even when SACCO data is accessible.					
7.	I am aware of the potential risks of using personal devices for work.					
8.	I believe that my personal device is more vulnerable to cyber threats than company-provided devices.					
9.	I am careful about the types of networks I connect to when using my personal device for work.					
10.	I believe that my device usage habits do not pose a significant risk to SACCO’s data security.					

SECTION D: LOCATION						
Please indicate the extent to which you agree with the following statement on Location usage on context awareness vulnerabilities in BYOD Environment.						
No.	**STATEMENTS**	**RATING**				
		(1)	**(2)**	**(3)**	**(4)**	**(5)**
1.	I frequently access SACCO systems from locations outside of the office.					
2.	I often connect to public Wi-Fi when working remotely.					
3.	I use a VPN or other security measures when accessing SACCO systems remotely.					
4.	I believe that accessing SACCO data from home is as secure as from the office.					
5.	I am concerned about the security of SACCO data when accessing it from public places.					
6.	The location from which I access SACCO systems affects the speed and reliability of access.					
7.	I am mindful of my surroundings when accessing SACCO systems in public.					
8.	I prefer working from locations where I can ensure secure access to SACCO systems.					
9.	I believe that SACCO should implement stricter controls for remote access.					
10.	I notice a difference in the security measures required based on my access location.					

SECTION E: ROLE RISK FACTOR						
Please indicate the extent to which you agree with the following statement on role risk factor on context awareness vulnerabilities in BYOD Environment.						
No.	**STATEMENTS**	**RATING**				
		(1)	**(2)**	**(3)**	**(4)**	**(5)**
1.	My role within the SACCO requires frequent access to sensitive information.					
2.	I have more access privileges than necessary to perform my job.					
3.	My decision-making authority impacts the level of access I have to SACCO systems.					
4.	I believe that employees in higher roles pose a greater risk to data security.					
5.	I receive regular cyber-security training specific to my role within SACCO.					
6.	I am confident that my role-specific access to SACCO systems is properly monitored.					
7.	I think employees with similar roles to mine should have restricted access to certain data.					
8.	The security protocols in place for my role are sufficient to prevent unauthorized access.					
9.	I believe that role-based access controls are crucial for SACCO's data security.					
10.	I am aware of the potential risks my role poses to SACCO's cyber-security.					

SECTION F: CONTEXT AWARENESS VULNERABILITY						
Please indicate the extent to which you agree with the following statement on context awareness vulnerability in BYOD environment						
No.	**STATEMENTS**	**RATING**				
		(1)	**(2)**	**(3)**	**(4)**	**(5)**
1.	I am aware of the potential security risks associated with using personal devices for work purposes					
2.	I understand how my device usage could potentially expose SACCO systems to cyber-security threats.					
3.	I am confident in identifying potential security risks when accessing SACCO data from different locations.					
4.	I regularly monitor my device for any unusual activity that could indicate a security breach.					
5.	I believe that my awareness of security protocols is sufficient to prevent context-related vulnerabilities.					
6.	I often consider the security implications of accessing SACCO systems from various locations.					
7.	I am aware of the specific vulnerabilities that may arise due to my role within the SACCO.					
8.	I actively take steps to minimize the risks associated with accessing SACCO data at different times of the day.					
9.	I am familiar with the measures SACCO has in place to address context-related security vulnerabilities.					
10.	I believe that increased awareness of context vulnerabilities could improve SACCO’s overall cyber-security posture.					