A MODEL OF BYOD INTEGRATION TO INCREASE CORPORATE INFORMATION SECURITY IN BANKS: CASE OF EQUITY BANK KENYA

BY

GLADYS MUNYAZI DALLA

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

SEPTEMBER, 2021

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.

NAME: Gladys Dalla REG. NO. 16/01840

Sign..... Date: 20/09/2021

This project has been submitted for examination with my approval as the appointed university supervisor.

Sign..... Date: 21/09/2021

Dr. Lucy Mburu

Supervisor

ABSTRACT

Bring Your Own Device or BYOD is a novel approach where employees and stakeholders in organizations bring their personal computer devices to the workplace. Employees are able to access organization information and data through their devices under the BYOD policy. On the other hand, the BYOD approach heightens the risk of malware attacks and therefore, diminishes the integrity of the information security within the organization. The current study sought to develop a model for the integration of BYOD in the banking sector while maintaining a sustainable corporate information security. The theories guiding the study are the technology threat avoidance theory and unified Theory of Acceptance and Use of Technology. On the other hand, the research study adopted a cross-sectional survey design to collect data. The survey design is effective in coming up with quantitative data that aids one develop inferences regarding a particular phenomenon. The study established that Mobile device management, Information security policies, Security culture and Employee education as BYOD factors have significant effect on Sustainable corporate information security. Following data collection the researcher was able to clean, code and analyze data using SPSS v27. An OLS model was derived from the analyzed data. The derived statistical model can be instrumental in integration of BYOD while maintain information security. The generated model was tested and validated through multiple regressions test statistics. The Adjusted R value obtained through model summary was r^2=0.437 indicating that the independent variables of Mobile device management, Information security policies, Security culture and Employee education contribute 43% variation in Sustainable corporate information security. The ANOVA statistic showed that the independent variables are significant to the dependent variable. Subsequently, the independent variables in the study have a significant impact on the dependent variable of Sustainable corporate information security. Moreover, the researcher recommends that organizations in the banking sector have a device register in the BYOD platform to ensure information security. The findings of the research are significant to the corporate sector as it adds knowledge that will help guide the security model employed in running BYOD. Integration of BYOD is a necessity in most industries, hence this research provides a robust model for heightening Sustainable corporate information security.

ACKNOWLEDGEMENT

First and foremost I give thanks to the almighty God for giving me sufficient grace. I extend my appreciation and gratitude to all those that contributed immensely towards completion of this research project. I am very grateful to my University Supervisor for her tireless assistance, high quality and keenness on details, experience and initiatives which guided me in enriching and completing this research project.

I owe a debt of gratitude to my family who sacrificed time and gave me invaluable support that saw me through the challenging period. A special thanks to my loving family who were especially supportive in listening to my thoughts and helped me work out logistical details throughout this process. In particular, I am grateful for the inspiration I have received from Miriam Njeri and Jesse Kiarie.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
ANOVA	Analysis of Variance
BYOD	Bring Your Own Device
MDM	Mobile Device Management
3G	Third Generation
4G	Fourth Generation
IoT	Internet of things
IS	Information Systems
IT	Information Technology
IBM	International Business Machines
MUSES	Multi-platform Usable Endpoint Security System
SPSS	Statistical Package for the Social Sciences
TTAT	Technology Threat Avoidance Theory
UTAUT	Unified Theory of Acceptance and Use of Technology
zIPS	Zimperium Intrusion Prevention System

GLOSSARY

Adoption and integration	Technology that has been accepted and put to use by an organization.
Cloud Computing	This is the delivery of applications and tools such as software, databases servers, storage etc. through the internet.
Endpoint Security	Endpoint Security refers to protecting the various end-user devices such as smartphones, laptops, or tablets. These endpoints serve as points of access to the corporate network and sensitive data.
Model	To create a representation of something on a small scale so as to base your predictions of the future outcome.
Mobile Technology	Technology that goes where the user goes.
Mobile Computing	Technology that allows transmission of voice, text and video through devices that are not connected using any physical link. These devices are portable and connected over a network. This is referred to as wireless communication.
Mobile Environment	This is the ability to access data or information while on the move. This can be done wirelessly or while physically connected to a device.
Machine learning	Machine learning is the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyze and draw inferences from patterns in data.
Regressions analysis	Regression analysis is a set of statistical methods used for the estimation of relationships between a dependent variable and one or more independent

	variables. It can be utilized to assess the strength of the relationship between variables and for modeling the future relationship between them.
Predictive modelling	Predictive modeling is the general concept of building a model that is capable of making predictions. Typically, such a model includes a machine learning algorithm that learns certain properties from a training dataset in order to make those predictions.

CHAPTER ONE

INTRODUCTION

1.1 Background

Organisations in the contemporary society have come to appreciate the rapid growth of information technology and its benefits to the company operations. The changes taking place through information technology support the use of portable computers and handheld smartphones. While some organisations are apprehensive about the use of personal computers in their networks due to data security, some have embraced the BYOD culture. The BYOD or Bring Your Own Device is a strategy where organisations allow employees and even customers to utilize their personal devices in undertaking organisational tasks.More organisations have embraced BYOD due to the flexibility it offers to the employees and the organisation in terms of working on projects and different tasks.

The BYOD phenomenon started once the Apple iPhone was introduced to the society back in 2007 (Zambrano & Rafael, 2017). Introduction of smartphones such as the iPhone brought about a revolution in the consumer technology sector. Handheld computer devices were a major hit for both employees and management since they could access their emails and other documents. Besides, consideration for BYOD expanded in 2009 when Intel Corporation recognized the benefits of employees working remotely or in mobile environment (Zambrano & Rafael, 2017). Furthermore, in 2011 software vendors such as the company Citrix system brought out new platforms that support the BYOD trend. The proliferation of mobile devices has led companies such as IBM to introduce BYOD solutions that focus on management of computer devices at the workplace.

The proper integration of BYOD requires supportive policies from the organisation coupled with resource availability. Many organisations globally are making considerable progress towards successful integration of BYOD. Organisations are increasingly providing the latest mobile and IT devices that

enable employee's access the resources of the company (Chao et al., 2020). The main objective of integrating BYOD into the organisation is to improve the level of employee satisfaction and their performance through flexibility in the workplace. On a different note, the continuous growth and integration of BYOD has led experts to review the corporate security measures associated with privacy and company documents. Concerns arise from the ability of employees to move with company information to their homes coupled with remote access to sensitive documents. Zambrano and Rafael (2017) assert that 80% of the organizations that have embraced BYOD have exhibited a significant increase in productivity. Moreover, over 360 million users of BYOD report that some of the benefits include heightened customer satisfaction and productivity within the workplace. Moreover, BYOD offers organizations an opportunity to lower their operating costs such as utilities sincemore individuals operate remotely. Organizations that embrace BYOD do so at varying extents since some organisations offer internet access and or computer devices to be used by the employees. Employees who have sufficient resources for BYOD adoption have more flexibility in the execution of their tasks as they can do so beyond the working hours.

The growth and use of BYOD continues to grow globally as more organizations and stakeholders appreciate the arising benefits. At least 85% of employees in India have adopted the use of smartphones in the workplace. Similarly, 76% of employees report using mobile computer devices to work on their tasks away from workplace. The rate of BYOD integration in USA stands at 55% while in the United Kingdom 38% of employees use mobile devices to work on tasks they are assigned by their employers. The use of BYOD culture continues to grow due to the technology innovations taking place every other day. Subsequently, the rate of BYOD adoption and integration will continue to rise as information technology continues to proliferate within the contemporary society.

BYOD is considered in the contemporary society as the new norm when it comes to business computing (Musarurwa et al., 2017). Subsequently, organizations that have an ambition to be consistent in terms of productivity in this era have a duty to review their BYOD security solutions. Information science has

become a multidisciplinary, multi-organizational and even departmental. Besides, organizational features have a significant influence in the performance of employee hence firms with BYOD integration tend to be more productive. The need to employ BYOD necessitates a culture of organizational information security. Moreover, a positive information science culture helps improve the attitude of employees towards the application of BYOD within the firm and supporting the security system available. Employee attitude towards BYOD can be positive or negative and determines the culture of the employees towards information science integration. Such an attitude is essential since it influences the policy framework and the regulations that surround the implementation of BYOD.

The attitude of employees is critical to a successful information science culture especially in respect to implementation of BYOD. On the other hand, the information science culture is dependent on the knowledge held by employees regarding information technology policies and compliance with the same. Employee knowledge on information science policies such as BYOD is essential since it affects the training on information science platforms (McClean, 2016). In the current context, knowledge refers to what the staff members know regarding BYOD platform within the bank coupled with what they know regarding the hardware that supports BYOD. Moreover, employees should be knowledgeable regarding the BYOD software that manages the platform, data present in the system and the policies that are necessary for optimal operation of devices.

Employee's operational knowledge of BYOD is critical as it ensures the information security during its use in any device. A good example, employees should be knowledgeable enough to avoid downloading software that can be malicious and detrimental to the BYOD (Jiunn-Woei, 2020). The operational knowledge of bank employees regarding BYOD policies and framework is integral to the security of data within the organization. Bank employees are normally hired based on the inherent knowledge that they hold for particular jobs within the company. Subsequently, the inherent knowledge can buttress the existing knowledge management initiatives undertaken within the organization.

Barlette et al., (2021) asserts that BYOD has been used for at least fifteen and has undergone major

changes. Initially, BYOD hardware included laptops and mobile phones; currently 90% of BYOD takes place using smartphones, connected devices and tablets. A second from of evolution involves the power of devices used and a higher rate of connectivity. Modern day smartphones have a high performance capacity of up to 10 cores which offers performance that nears that of low-end laptops. Furthermore, connectivity has improved significantly through hi-speed Wi-Fi and Bluetooth. Subsequently, elaborate applications used by employees including emails and ERPs can be accessed through personal devices more easily. Barlette et al., (2021) asserts that cloud-based applications provide storage of data that is essential to the organization. Moreover, contemporary operating systems have moved from proprietary systems to secure democratized platforms such as Android.

The growth in technology, accessibility and connectivity has improved the operations undertaken and enabled growth of BYOD. Barlette et al., (2021) asserts that organizations using BYOD are able to generate annual savings of up to $ 350 per employee. Besides, the use of personal devices heightens productivity by at least 34%. The main threats posed by the use of BYOD largely involves data leakage and further malware infiltration. The year 2017 saw employee personal devices contribute 51% of data breaches. Computer breach endangers the firm and further allows illegal access to the corporation's external partners through digital connection and this heightens the vulnerability to potential cyber-attacks. The laws and regulations established to protect computer platforms have failed to safeguard BYOD in organizations. In fact, only 40% of workers are under regulations that guide on the use of personal devices.

It is imperative for organizations such as banks to improve their security regulations considering the high integration of BYOD within banks and other vital organizations. The use of BYOD is prevalent among employees and sometimes they do so without any set regulations to protect against such a breach. Most employees hold an individualistic view on the benefits of BYOD and their perception on information security is geared towards privacy of their personal information. On the other hand, managers are compelled to consider the security of the entire platform as they seek to attain the

objectives of the organization. Managers are in most cases forced to employ reactive measures once there is a security breach in the BYOD platform rather than regulate the use by employees (Barlette et al., 2021). It is difficult for bank management prohibit the use of personal devices since they do not own such items but rather the employees have freedom to the devices. Consequently, it is essential to have a robust strategy and plan on how to manage the BYOD platform and capture the benefits and opportunities it presents while mitigating the risks.

BYOD integration in any organization requires adequate software and hardware resources that support the information system. It is imperative that companies seeking to integrate BYOD develop a robust financial and sustainability framework that will ensure the information technology platform has enough resources to ensure it supports the needs of the organizations (Chalee et al., 2017). A good IT plan on sustainability will ensure that BYOD adoption is reliable and supports the needs of the employees and the organization. Besides, the amount of productivity realized under BYOD ensures that more organizations are interested in integrating the information system platform into their daily operations. The continuous improvement of resources needed for BYOD is essential in financial organization which need to protect their information data. The integration of BYOD alters the business processes and practices leading to a lean structure that is more manageable for the employees and the organization at large.

Integration of BYOD presents different opportunities and benefits that banks and other organizations can benefit from through heightened productivity. BYOD use in the different organizations is associated with increased motivation in the workforce, satisfaction levels increase while performance and innovation improves (Lawrence, 2018). Adoption of BYOD by employees contributes to efficient assimilation, efficient use while employees can adapt their workplace tasks. Moreover, BYOD is associated with improving interactions among employees coupled better recognition among the workforce leading to employee retention. Moreover, organisations stand to benefit from the integration of BYOD in their daily operations and strategy. BYOD offers vast innovations and platforms that

employees can use to promote the mission and vision of the organization (Lawrence, 2018). Social media is one platform that organisations are able to market their products through. BYOD ensures that employees can be involved in the process. Moreover, BYOD brings together the employees into a singular platform where communication is shared and records kept for reference.

1.2 Statement of the Problem

The banking sector is highly dynamic in Kenya amid changes in government policy and growth in information technology access in the country. Government policy has shifted towards cheaper interest rates in the financial services sector and this will erode the profit margins of banks. On the other hand, the growth in information technology systems has led to enhanced access to mobile financial services for the average citizen. Subsequently, banks are forced to adopt novel ways of coming up with services and products that will attract more customers every day. The prevailing challenges in the banking sector necessitate better digitization of the operations coupled with better response to customer needs. BYOD offers banks a mutually beneficial option for enhanced productivity and better customer service. Consequently, BYOD is an integral element in the banking sector and it will continue to grow.

On the other hand, the security of customer data and information in the banking sector faces multiple threats including malware attacks and computer hacking leading to theft of funds in the bank accounts. Multiple studies on BYOD indicate the security risks associated with BYOD adoption in an organisation (Boysen et al, 2019; Jiunn-Woei, 2020; Nalin & Love, 2014). Saxena et al., (2020) asserts that the cost associated with insider computer threats increased by at least 31% to $ 11.5 million between 2018 and 2020. Similarly, the occurrence of malicious interference of corporate networks spiked by 47%. Previous models proposed by (Veljkovic & Budree, 2019; Zamhariah, 2018) fail to expound on how banks can adopt BYOD and retain a sustainable corporate information security culture.

Zainab et al., (2017) advances new BYOD model based on a fuzzy-Analytical Hierachy Process to be used in different organizations. The BYOD model proposed fail to consider the unique needs of the

banking sector. On the other hand, Cuevas et al., (2015) proposed a model known as the Multi-platform Usable Endpoint Security (MUSES) for securing and managing BYOD environments. The model uses machine learning and computational intelligence techniques. The model used by Cuevas et al., (2015) lacks the capability to integrate the analysis of users through social networks. Subsequently, the platform cannot ensure security of user's data when they are engaged in social networks. The knowledge gap will be filled by the current research that examines the banking sector in Kenya. Moreover, recent events Including the Sars-Cov 2 (Covid-19) pandemic that requires social distancing have led to heightened use of digital platforms to communicate and work. Subsequently, BYOD adoption will continue to grow and this requires a model that will enhance corporate information security.

The current study is geared towards addressing the information gap regarding the development of a BYOD model that ensures a sustainable corporate information security in the banking sector in Kenya. The model seeks to ensure customer data, information and funds are safe within the banks even when personal devices are in use by the employees.

1.3 General Objective

To establish a model for BYOD integration to increase corporate information security in banks.

1.4 Specific Objectives

i. To review the corporate information security challenges arising from the integration of BYOD in the Banking sector.
ii. To examine the factors of BYOD integration that affect a sustainable corporate information security.
iii. To develop a BYOD model using the identified influential factors.
iv. To test and validate the model.

1.5 Research Questions

i. What are the corporate information securities challenges arising from the integration of BYOD in the Banking sector and the mitigating measures to overcome them?

ii. Which factors of BYOD integration affects a sustainable corporate information security culture in the banking sector?

iii. What is the appropriate design for a BYOD model in the banks?

iv. Will the developed model for BYOD security be suitable in improving the corporate information security in banking sector in Kenya?

1.6 Significance of the Study

This study was conducted at a time when working from home had become a norm and employees interacted with corporate information from their personal mobile devices more frequently. Employees working from home are at a much greater risk than if they were working from the offices. Cybercriminals have an easier entry into the company network through their mobile devices, since home connections are less secure. These blurred lines between personal and professional life increase the risk that sensitive information will fall into an insecure environment. It is fundamental to understand the security implications this would bring about to a bank. CISO's Benchmark Report 2020, indicates that organizations are struggling to manage mobile devices of employees working from home. The biggest challenge for these organizations remains how to successfully integrate BYOD while at the same time ensuring that the security of information stored in their information systems is not compromised (Namisiko, Sakataka & Sugut, 2015). The study findings and conclusion will help the bank security professionals analyze and better understand the prevailing features and threats of BYOD in the corporate sector. Subsequently, security professionals will be able to set up BYOD systems that can mitigate such arising threats.

The banking employees will benefit from the study as it will provide solutions to the challenges BYOD integration brings about which they face on their daily mobile device usage with corporate information.

They will be aware of what they are required to do and know so as to ensure the implementation and use of personal mobile devices to access corporate data is a success and beneficial to the company and their clients.

Moreover, the study will add knowledge to the field of corporate information security in a dynamic information technology environment. The findings will therefore form a basis for future studies in the area. The model developed will influence the security established in the integration and use of BYOD in banks. In this regard, the model developed will help safeguard the information and data of banks that allow the use of BYOD by employees.

1.7 Motivation of the Study

BYOD has been identified as a model that will continue to grow as more organisations appreciate the benefits such a strategy offers. Subsequently, more employees will seek to use their personal mobile devices to access the organizations information and data (Jiunn- Woei, 2020). The information security risks associated with BYOD are significant and can hinder the successful integration of BYOD in the banking sector. The realisation that BYOD is now more than just a policy or technical issue but rather an issue that is an integral part of the overall information security strategy for organization mainly banking sector as they have a high information security risk involvement, motivated the theme for this paper.

This study offers to develop a model that will enhance the integration of BYOD while ensuring a corporate information security culture. BYOD is indispensable in the banking sector as the firms seek to offer real-time financial services to the customers. Subsequently, the model can be integrated within the banking sector to ensure better productivity within the workforce. Development of a model that incorporates the risks associated the use of BYOD is essential as it will guide the integration among employees in the sector. Furthermore, the BYOD model will inform on the best security measures that banks should set-up to mitigate against loss of crucial data.

1.8 Scope of the Study

The scope of the study is limited to organizations operating within the Kenya banking sector. Subsequently, the study will focus on Equity bank as the main organization whose employee population will be targeted for data collection. The bank was chosen since it has a significant share of the banking sector in the country. Subsequently, findings from the study can be utilized to explain the events surrounding BYOD use in other banking institutions.

CHAPTER TWO

LITERATURE REVIEW

2.1 BYOD Integration Overview

The concept of Bring Your Own Device (BYOD) arises from the notion of cloud computing and mobile device use. From the beginning of the year 2006, the corporate world realised the significance of Smartphone's and their use in organisations. On the other hand, the growth in information technology consumerism over the recent past has allowed and promoted the emergence and growth of BYOD to become a significant IT consideration. Consequently, the adoption of BYOD is no longer a question of whether it will be integrated into organisations but rather a question of readiness on the part of firms (Veljkovic & Budree, 2019). The integration of BYOD by different organisations has allowed many enterprises to heighten the level of efficiency and quality of work, convenience and brought down the costs associated with management of IT infrastructure.

BYOD adoption allows employees to use their mobile communication devices to the workplace to help undertake tasks of the corporation. The use of BYOD is primarily driven by the user's preference rather than an initiative driven by the organisation (McLean, 2016). Some of the users who push for BYOD use are the employees who seek to access company information while at home or in a mobile environment. Subsequently, under the BYOD system, employees, business partners and even customers can easily access organization information through a web browser using a device that is not managed by the firm. The ease of access for information brings about security risks including data theft and leakage (Chalee et al., 2017). On the other hand, the use of BYOD continues to grow due to the many benefits associated with the strategy.

The proper integration of BYOD requires supportive policies from the organisation coupled with resource availability. Many organisations globally are making considerable progress towards successful integration of BYOD. Organisations are increasingly providing the latest mobile and IT devices that enable employee's access the resources of the company (Chao et al., 2020). The main objective of

integrating BYOD into the organisation is to improve the level of employee satisfaction and their performance through flexibility in the workplace. On a different note, the continuous growth and integration of BYOD has led experts to review the corporate security measures associated with privacy and company documents. Concerns arise from the ability of employees to move with company information to their homes coupled with remote access to sensitive documents.

Information systems that incorporate big data within the business operations are associated with smart and efficient operations. Moreover, the adoption of BYOD in organizations helps support the use of big data by employees and different stakeholders. One critical issue that arises with the use of BYOD in the current era of smart devices remains how safeguard the business information security. The availability of cloud computing technology and smart devices has heightened the adoption and integration of BYOD (Jiunn-Woei, 2020). The continued use of mobile devices in the workplace has brought about significant security challenges coupled with greater awareness of the prevailing risk management issues within the organization (Liang & Xue, 2009). Moreover, the trend correlates with increased investments in the security of technology.

The security threats associated with BYOD use have a negative impact on its diffusion and adoption due to multiple factors. Network protection under BYOD platforms is complex due to the ability of the devices to connect to multiple types of networks (Palanisamy et al., 2020). Employees use smartphones more regularly to access the BYOD platform yet the devices are connected to different applications and digital services that may pose a risk to the information system. Similarly, cloud services accessible through smartphones are at risk from malware due to their nature of being accessible to multiple users. In addition, cloud administrators can undertake unauthorized access which is detrimental to the organization data integrity. The introduction of IoT and connectivity with different devices has heightened the risk of information security since most devices are poorly secured by their users.

Furthermore, the use of personal devices as part of BYOD integration comes with the risk that devices

are stolen or lost by the employees. Such an event would jeopardize the organizational data since cybercriminals find smartphones as an easy target. Corporate data in an employee's smartphone is at risk when a smartphone with authorization codes is stolen or illegally accessed by cybercriminals (Palanisamy et al., 2020). The risks associated with personal device use heighten when the employee fails to adhere to the organizational and compliance policies. It is difficult for the organization to monitor the daily usage and compliance by the employee. The main priority of the employee is to protect their own data and information and may care less about the bank information and data. Furthermore, privacy-protective controls in the settings of the personal devices may be difficult to access and this deters employees from using them appropriately. Subsequently, acts of omission or commission by the employ can be responsible for data breach through the BYOD system integrated I the bank.

The traditional information systems environment supports the use of cloud computing and broadband internet that is essential for BYOD integration. Such resources further enable BYOD stakeholders to access big data from the mobile environment and there is no time limit for such access. Subsequently, the risk of data breach becomes higher under a BYOD setup compared with the traditional information systems environment (Nalin & Love, 2014). The use of BYOD in the workplace permeates the boundary between personal and corporate computer devices hence creating a challenge in securing information. BYOD, therefore, is associated with high-security risks within the business organizations and its adoption and processes are significantly different from the traditional information systems.

The protection of company information security is a critical issue that relies on control and management of the technology platforms coupled with user behaviour (Dawson & Thomson, 2018). The security risks associated with the cloud computing environment has heightened the need to manage information security issues associated with BYOD. Some of the strategies adopted in securing information under BYOD include data security and device management in different organizations. BYOD information security awareness is

below what is required and the users need to be constantly reminded. Similarly, BYOD is utilised within smart business environment where deep learning, Internet of Things, and cloud computing are the basic elements. Such information technology applications and platforms are new technology advancements that are associated with privacy, security risks (Ahmed et al., 2017). Besides, some forms of information security threats associated with use of BYOD include Distributed Denial of Service attacks, data leaks and malware (Olalere et al., 2015). Subsequently, security of information is a significant determinant for BYOD integration within the operations of an organization.

Integration of BYOD offers a myriad of opportunities and benefits that banks and other organizations can benefit from through heightened productivity. BYOD adoption in different organizations is associated with increased motivation in the workforce, satisfaction levels increase while performance and innovation improves (Lawrence, 2018). Adoption of BYOD by employees contributes efficient assimilation, efficient use while employees can adapt their workplace tasks. Moreover, BYOD is associated with improving interactions among employees coupled better recognition among the workforce leading to employee retention. Moreover, organisations stand to benefit from the integration of BYOD in their daily operations and strategy. BYOD offers vast innovations and platforms that employees can use to promote the mission and vision of the organization (Lawrence, 2018). Social media is one platform that organisations are able to market their products. BYOD ensures that employees can be involved in the process.

The use of BYOD and social media can be facilitated when employees are actively involved in improving and further rethinking some aspects of the firms processes (Barlette et al., 2021). The main advantage to the integration of BYOD is the fact that it enhances the communication between employees. Besides, it helps enhance the organizational culture regarding information sharing and marketing. On the other hand, organizational costs associated with BYOD integration are minimal since the devices are owned by the employees and costs associated with their management lies on the users. In

this regard, integration of BYOD in banks ensures heightened productivity due to morale boost and performance coupled with cost savings.

Due to the nature of BYOD platforms benefits and risks, it is imperative that managers review the use by employees. It is imperative that management offers top-management support for the integration of BYOD within the organization. Subsequently, resources must be provided for the protection of the BYOD platform by management. Changes must be implemented consistently to ensure that the organization benefits from BYOD while mitigating the associated risks.

2.1.1 Elements of BYOD

BYOD is more often described based on its different elements including mobility and risks. Mobility describes mobile individuals, mobile equipment, mobile environment and cloud computing. The aspect of mobility describes the fact that the user is not tied to any particular geographical location and further making the information and data generated available every time it is needed by users within the organisation (Veljkovic & Budree, 2019). Organisations that provide BYOD devices and resources do so with a view of heightening productivity and mobility among the employees. Mobility among employees allows flexibility in their daily operations and this ensures that they become more productive.

On the other hand, the element of mobile individuals refers to individuals in movement even though such a description defines every person in society. In the context of organisations, mobile individuals define employees who work remotely with a view of achieving the objectives of the organisation (Palanisamy et al., 2020). Mobile individuals are moving in space and their information is generated from their environment and surroundings where they operate and interact. Subsequently, the mobile individuals will more than likely use personal devices on their everyday operations and roles.

Similarly, the element of mobile environment refers to a situation where people are in motion but are on a personal level stationary. Mobile environments in the contemporary society include airplanes, trains and motor vehicles that transport the individual. Subsequently, the stationary individual may seek to work from

their position on transit with a view of completing particular projects and BYOD facilitates such objectives (Disterer & Kleiner, 2013). The mobile environment facilitates the employees to become productive while using their mobile technology for the organizations benefit.

BYOD Elements	Examples	Source
Mobile Individuals	Employees working remotely	Palanisamy et al., 2020
Mobile Environment	Aeroplanes. Trains and Motor vehicles	Disterer & Kleiner, 2013
Mobile Computing	Mobile Routers	Jiunn-Woei, 2020
Cloud Computing	Microsoft Office 365; Dropbox	Veljkovic & Budree, 2019

Table 2.1: BYOD Elements

Mobile computing is an essential element of BYOD concept as it describes technologies that support people's access to network services from any location. Mobile computing includes technology that facilitates transmission of data, video and voice through a computer or other devices with wireless capabilities (Jiunn-Woei, 2020). Subsequently, one does not need to be connected through a fixed physical link. The adoption of BYOD by any organisation requires a robust mobile computing platform for successful implementation. Similarly, cloud computing is another significant element of BYOD in organisations. Cloud computing is a cost-efficient alternative for the management of complex systems in IT. Many organisations are taking advantage of cloud computing services such as Microsoft Office 365 and Dropbox storage to facilitate productivity of employees under BYOD.

2.1.2 BYOD Global Adoption

The concept of BYOD was first discussed in the early 1990s but its use has become prevalent after the surge in smartphone use in 2011 (Jamal et al., 2019). Adoption of BYOD is facilitated by the high number of individuals using smartphones which has a high computing power. The use of mobile phones is high since at least 10 billion devices were in the market and used exceeding the world population. Consequently, the adoption of BYOD is a necessity since employees are using personal computing

devices regardless of whether the organization itself has regulations on management of such devices. Moreover, a majority (69%) of employees report using smartphones and tablets at the office. Subsequently, prudent managers have adopted the use of personal devices at the workplace in order to maximize on the available information technology resources. Organizations are increasingly appreciating the benefit that comes from using BYOD technology while at the same time they worry about the risk and threats to their organizational data.

In the past decade significant changes have taken place within the IT world especially involving hand-held mobile devices. According to Zainab et al. (2017) a meagre 17% of consumers had smartphone's by the year 2009 as compared to 81% by the year 2016. Moreover, other significant trends that support BYOD have taken place in the recent past including a rise in the use of IoT and wearable device technology. The growth in technology has made available hand- held devices that have a strong wireless connection with other devices. Consequently, it is now easier for employees and organisations to connect remotely from any part of the globe (Zambrano & Rafael, 2017). The rate of mobile device adoption in a country or region is a determinant of how well BYOD has been integrated. BYOD adoption and integration ensures and allows employees to use their mobile communication devices at the workplace to help undertake tasks of the corporation. The use of BYOD is primarily driven by the user's preference rather than an initiative driven by the organisation (McLean, 2016). Some of the users who push for BYOD use are the employees who seek to access company information while at home or in a mobile environment. Subsequently, under the BYOD system, employees, business partners and even customers can easily access organization information through a web browser using a device that is not managed by the firm. The ease of access for information brings about security risks including data theft and leakage (Chalee et al., 2017).

Countries such as South Africa have shown a high degree of BYOD integration due to the rate of mobile device adoption. South Africa reported 37% adoption of Smartphone's by the year 2016. Subsequently, BYOD is highly accepted within such a nation. Similarly, the BYOD integration in Malaysia stood at

85% by the year 2018; 26% of the employees reported being provided with enough facilities for BYOD by their IT department (Zamhariah, 2018). Some of the devices widely used for BYOD in Asia-pacific region include laptops, tablets, and Smartphone's. Cisco conducted a survey on BYOD prevalence in eight nations and concluded that it is now a global phenomenon. The regions covered in the survey include Europe, Latin America and Asia (Olalere et al., 2015). Moreover, 75% of employees in emerging economies of India, Singapore and Brazil utilize BYOD in their workplaces. On the other hand, 44% of employees use BYOD in developed nations such as Italy, Japan and Sweden.

Jamal et al., (2019) asserts that adoption of BYOD emanates from the fear by managers that risks associated with it exceed the benefits. Previous research show that organizations found the concerns for management regarding BYOD adoption to include: security attacks as most concern (32%), malware (29%), data leakage at 14% which was followed by risk of stolen device (12%), DDOS attack was at 5% while the least concern was unauthorized software or bandwidth challenge (1%) (Jamal et al., 2019). Subsequently, organizations require robust security measures and policies to ensure that the information technology platform is well protected. Some of the options available include knowledge based solutions, biometric-based, possession-based authentication. Such measures can be used in managing the BYOD platform but the main risk remains to be with the centralized storage which can be vulnerable to attacks (Lawrence, 2018). BYOD adoption requires a culture of developing BYOD protection measures that can detect cases of data leakage and also prevent security attacks. It is imperative that organizations institute measures that offer novel security measures and further protection of the users and organizational data.

Adoption of BYOD in different organizations heightens when there is a reliable policy and regulations guiding its use by employees. Subsequently, a robust BYOD policy must specify the personal devices allowed within the organization (Dawson & Thomson, 2018). The four main categories of personal devices that should be described in the BYOD policy include standard, internet ready, borderline or an amalgamation of both categories. Moreover, the category of devices stipulated in the BYOD policy

depend on the technical support level provided by the organization. Similarly, instructional focus by management and compatibility of devices determines the policies and regulations that guide the BYOD platform. Previous research shows that most BYOD policies favor an internet-ready devices when using the BYOD system. On the other hand, Dawson and Thomson (2018) assert that BYOD adoption is lackluster when the policies are geared towards a more technical supported system and management-directed close guidelines which requires standard devices. The benefit of standard devices is the fact that it is easier to employ desired security configurations and software updates on standard devices compared to different devices with individual operating systems.

Adoption of BYOD has been found to be especially beneficial since it improves the technology knowledge and acceptance within the organization (Cuevas, 2015). Moreover, the adoption of BYOD in institutions is favored by heightened efficiency and ability to cover the initial learning curve. Besides, using standard devices ensures that employees and stakeholders in the organization are able to undergo a smooth learning curve. Employees with hectic schedules and deadlines can benefit from using familiar standard devices under the BYOD system hence improving the amount of time and energy one can put on the main task. Moreover, the features of potential adopters, innovation available and local context determine the level of technology adoption within the organization. Lawrence (2018) asserts that BYOD adoption improves when the people involved are innovative and with a high rate of computer self-efficacy. Besides, superior innovations and personal devices that are user-friendly and compatible with daily tasks will help improve BYOD adoption in banks and other institutions.

BYOD adoption can heighten the engagement by employees in the workplace and contribute towards more productivity and better efficiency (Cuevas, 2015). Subsequently, BYOD has become an indispensable technology that employees in banks can use to heighten their efficiency and realization of the corporations goals and objectives. Research by Lawrence (2018) asserts that BYOD adoption is dependent on the nature of potential adopters, the features of the organization and the available

technological innovation. Some of the individual factors highlighted by the researchers include personal innovativeness, gender, anxiety, education, attitude and motivation. Moreover, the perceived usefulness, complexity, observability, relative advantage are considered essential factors for any adoption by institutions and stakeholders to take place.

On the other hand, the research by Lawrence (2018) identified performance expectancy as a key factor that contributes towards adoption of BYOD. Performance expectancy refers to the degree to which potential adopters expect their individual performance to show improvement when they adopt a particular technological innovation. Besides. The research established that performance expectancy during adoption of BYOD integrates the perceived usefulness associated with technology acceptance model; extrinsic motivation, relative advantage associated with innovation diffusion theory and the outcome expectations that correlates with social cognitive theory. Furthermore, the behavioral intention of BYOD adopters is influenced significantly by performance expectancy. Similarly, the potential adopters hold a level of effort expectancy which helps determine whether the innovation will be user-friendly. Subsequently, potential adopters of BYOD consider the ease of use and the perceived ease of use in determining whether they will utilise the amenities availed by BYOD systems.

2.1.3 BYOD Adoption in Kenya

The rapid growth of IT infrastructure in Kenya has facilitated the uptake of BYOD by different organizations including banks and learning institutions (Arwa, 2014). The enhanced competition in the communication services sector has brought about the best in services for Kenyans. Companies such as Safaricom and Telkom Kenya offer fast internet connectivity through 4G+ networks. Subsequently, more Kenyans use personal mobile devices while in a mobile environment. Moreover, employees in different organizations have sufficient internet resources to undertake their daily tasks while on the go. Kenya is global leader when it comes to the growth and development of information technology adoption. The country is a leader in the number of people connected to mobile devices coupled with internet

penetration. Telecommunication companies such Safaricom have introduced advanced financial technology applications for transfer of money between users. Moreover, there has been tremendous investment in the youth through direct investments to new projects through incubation hubs.

The continuous growth of technology adoption in Kenya coupled with a population where the youth are the majority. Subsequently, the young generation that now works in different organizations has brought mobile devices to the workplace (Zainab et al., 2017). Organizations in the contemporary Kenyan society have integrated technology and connectivity to capture the benefits associated with use of information technology. Top management in different Kenyan organizations have identified the need to utilize technology in the daily operations of the workforce and further ensured that employees can use personal devices. Subsequently, the adoption of BYOD in different organizations including banks continues to heighten and this helps improve productivity. Organizations in Kenya have adopted BYOD because it offers improved productivity and efficiency in the workplace (Zainab et al., 2017). Similarly, Kenyan organizations have realized that BYOD offers much needed flexibility at the workplace unlike the traditional working hours. Moreover, the use of BYOD is associated with employee morale.

2.1.4 Factors Influencing BYOD

The use of mobile devices by employees under the BYOD concept is beneficial to both the company and the individual (Musarurwa et al., 2017). Corporations benefit by having access to their employees at any time of the day. On the other hand, employees benefit from a flexible working environment. BYOD integration and success heavily relies on the available IT infrastructure within the organisation. The computer hardware available for the employees is a critical factor that promotes or limits BYOD. Different devices can have operating systems that may not be compatible with each other and this affects the working capability of the employees using BYOD. Some documents developed using one operating system may fail to open in a different operating system. Similarly, the wireless internet speeds are essential for successful BYOD implementation (McLean, 2016). The higher the internet speeds the better the

connection for the users. Subsequently, access to 3G+, 4G+ or 5G+ internet speeds promotes faster remote connection for video conferencing and sharing of files among employees and the organisation.

Security and privacy has been identified as a significant factor that determines adoption of BYOD. Organizations that fail to adopt BYOD opine that security of their information is paramount and that they do not seek to have any loss of such information. Moreover, user acceptance of the mobile services is determined by the perceived security of the data. Besides, cloud services that support BYOD face a myriad of challenges including standardization, security and privacy (Arpaci, 2015). Other factors that affect the adoption of BYOD in corporations include perceived financial cost of the system and its compatibility with existing software.

Weeger, Wang, Gewald, et al. (2020) asserts that in the contemporary working environment, the young generation of staff are supportive of the integration of BYOD. The young individuals appreciate the potential benefits associated with BYOD programs. Subsequently, the demographic of employees that a corporation has in its workforce affects the integration and use of BYOD. On the other hand, the generation of young employees are more likely to download and install software that may prove risky to the organization network. Private devices that employees use under BYOD can lead to a massive attack once the users download and install multiple software for private use. The study by Weeger et al. (2020) indicates that employees using their personal devices at the workplace fail to consider the risk of exposing the corporate network to malicious software. Consequently, the individuals reap the benefits of using their own devices at work while the corporation is exposed to further risks. A young workforce is more likely to adopt BYOD in the organization but this requires a structured BYOD program to protect the corporation network.

Perceived risk of BYOD is a significant factor that influences the adoption of the practice in the corporate world (Lawrence, 2018). Corporate management hold a belief that extended exposure of the company data can lead to loss of the same. All forms of innovations are associated with the risk of losing valuable

assets. The inability to manage such risks can fuel the loss of data but an organization with a structured program on use of BYOD is able to counter such risks. The concept of perceived risk is associated with the perceived financial risk of setting up a BYOD program; perceived threats of data loss and perceived time risk. The apprehension of using BYOD can be linked with the repercussions of having to use the computer devices while at work and at home. Individuals are more likely to adopt innovations that are seen as having fewer risks. BYOD has a significant risk factor of data loss or malicious attack and this may deter employees from using the innovation.

The different innovations that have been developed for the consumer market have continued to find a way into the corporate workspace. Such an eventuality arises from the employees going to work with such products as they seek to capture their benefits. Subsequently, such actions have contributed towards the management of organizational data and daily tasks. In addition, information technology platforms such as social media, blogs and podcasts have affected the adoption of BYOD in the organization. The experience employees have in using particular technology can be harnessed by organizations to their own advantage. Consequently, the ease of use of the technology by employees is an important determinant of how BYOD is integrated into the organization (Cuevas, 2015). Traditionally employees are reluctant to accept new technology availed by the organization IT department. Most employees consider such a technology to be a form of replacing their services. On the other hand, technology introduced by employees into the organization is widely accepted. Employees share information on the best technology to use for communication and interaction. Subsequently, once such devices are introduced for organizational tasks, the employees are quick to learn how to use it and interact with each other. It is imperative that management in every organization identify the low hanging fruits that can be used to develop the productivity of the organization.

Besides, employees consider new IT products introduced by the management as being inadequate for the different tasks they have to undertake. Most employees who have used particular technology

privately and found it to be highly beneficial want the same experience when handling organizational tasks (Lawrence, 2018). Employees in such situations believe that such IT infrastructure can help fulfill their individual and collective objectives that are within the organization. The interactions of the employees with their personal devices continues to erode the boundary between private tasks and organizational objectives. Subsequently, employees are more likely to adopt BYOD once they know that they will be using familiar devices to undertake their daily functions. On the other hand, managers and the organization do not have to train employees on use of personal devices hence saving funds. In addition, the current generation of young employees prefer to work from mobile locations and do not want to limited by location. Mobility and flexibility is an essential need for the young generation of millennials who form a majority of the workforce within the different organizations. Furthermore, the Covid-19 pandemic has made working from home more fashionable and suits the integration of BYOD for the young employees.

Similarly, the development of reliable policies and regulations for managing the BYOD platform contributes towards adoption of the IT system in the workplace (Barlette et al., 2021). The establishment of policies empowers the employees to determine the best personal devices to use in the organizational tasks. Besides. BYOD regulations and policies encourage the staff to be more flexible and creative when managing their duties. The enactment of reliable policies guiding the use of personal devices in the organization ensures that resources are added to the organization without having to spend funds on the same. Furthermore, policy enactment for BYOD is essential since it facilitates proper risk management which is critical for security of the data within the organization.

However. BYOD adoption requires adequate software and hardware resources that support the information system. It is imperative that organizations seeking to integrate BYOD develop a robust financial and sustainability framework that will ensure the information technology platform has enough resources to ensure it supports the needs of the organizations (Chalee et al., 2017). A sound plan on

sustainability will ensure that BYOD adoption is reliable and supports the needs of the employees and the organization. Besides, the amount of productivity realized under BYOD ensures that more organizations are interested in integrating the information system platform into their daily operations. The continuous improvement of resources needed for BYOD is essential in financial organization which need to protect their information data. The adoption of BYOD alters the business processes and practices leading to a lean structure that is more manageable for the employees and the organization at large.

BYOD adoption is a clear manifestation of Information technology consumerization (Jang-Jaccard & Nepal, 2014). The more technology develops the more users come up with ways to maximize benefits from the technology. Subsequently, technology adoption continues to improve as more benefits are realized by the users. Novel IT products heighten the level of information flow in the society and this contributes to improved business processes. Subsequently more organizations are aligning themselves with new technology platforms such as BYOD. Besides, the banking segment has shown tremendous growth in terms of integrating technology. Bank managers have realized the benefits of using financial technology platforms to communicate with their customers and further promote their services. In addition, banking institutions offer customers products that are accessible through online services. Such necessitates the banks to link their employees with the organization IS platforms to ensure that they are productive and offer timely services to their customer population. The Constant threat of losing vital data exists but managers and other leaders in the organizations have accepted the challenge. Moreover, private institutions such as IBM have developed software and hardware products that can help avoid or mitigate against loss of customer information. Subsequently, the risk of losing data to third parties will continue to be managed going forward.

2.2 Theoretical Framework

The following section of the study highlights the BYOD adoption models and Machine learning techniques

and models that are consistent with the study objectives.

2.2.1 Technology Threat Avoidance Theory

The theory of Technology threat avoidance helps explain how users of IT platforms behave in order to avoid threats to their IT infrastructure. The TTAT differs from other IT security models as it considers the individual user instead of the organization as a whole. TTAT was developed by Liang and Xue (2009) after an extensive process of synthesizing literature from different fields including healthcare, information systems, psychology and risk analysis. Consequently, the main basis for the theoretical model is the fact that when individual IT users believe that an IT threat exists in their environment, they will become motivated to avoid the threat by undertaking safeguard measures. Moreover, when they believe that the threat cannot be avoided through the safeguard measures, they will undertake passive avoidance of the threat through a process of emotion-focused coping.

Subsequently, TTAT helps elaborate the factors and process that influence individual users behaviour in regards to threat avoidance. Besides, the theory posits that IT users behaviour towards threat avoidance can be illustrated through a cybernetic process where users intentionally enlarge the space between existing security state and the unsafe and undesired end state (Liang & Xue, 2009). The TTAT theory provides that users of IT devices as is the case under BYOD; experience two forms of cognitive processes that include threat appraisal coupled with coping appraisal. Similarly, IT users are quick to assess the security of their IT platform and devices and then decide which action is required to help avoid the threat. The users consider the probability of the IT threat taking place and the negative effects associated with the threat. Conversely, the IT users while determining the safeguarding measures will consider the effectiveness of mitigating actions, costs associated with the safeguard and self- efficacy of applying the identified safeguard measures.

The TTAT model provides knowledge and guidance in the application of BYOD in an organization and

corporate information security. Accordingly, avoidance of malicious threat by IT users acts as a form of dynamic positive feedback loop which may start by the existence of a malicious threat within the working environment. Subsequently, once the threat is identified the users establish an anti-goal which refers to being harmed by the IT threat. Besides, once it is apparent that the current state is closer to the undesired state, the users will engage in specific coping mechanisms with a view of enlarging the difference between current state in the IT platform and the undesired end-state of IT insecurity (Boysen et al., 2019). The behavior of threat avoidance will continue until the threat is significantly reduced that it does not serve as a challenge. TTAT model can be adopted in the organisations using BYOD strategy as a prescriptive guideline to corporate information systems security.

Carpenter et al., (2019) asserts that the ability to understand the individual threat avoidance motivation and corresponding behavior is an essential component when one seeks to design an effective cyber security solution. Such a strategy ensures that the cyber-security solutions are in tandem with the needs of the users and organization. According to Carpenter et al., (2019) individual's perceptions in regards to their susceptibility technology threats heightens their perception towards the threat in the system. Subsequently, the users are influenced by the threats and this affects their level of motivation and behavior to avoid or overcome the threats. The TTAT avails a logical and cogent explanation for individual's behavior towards technology threats. Threat perceptions have been evaluated through empirical tests and have provided robust findings on the influence of threats on the users. Carpenter et al., (2019) asserts that TTAT fails to account for the arising individual differences. Such differences include but are not limited to distrust propensity, risk propensity, coupled with impulsivity that has previously shown to influence information security behavior.

Similarly, Carpenter et al., (2019) asserts that perceived susceptibility towards technology threats is a major determinant of threat perceptions. The aspect of severity perception has partial mediation on the technology threat effect. Subsequently, the technology threat avoidance theory can explain the

discrepancy between approach-avoidance. In this regard, the theory proposes that avoidance of any malicious threat in technology is dissimilar to the adoption of a robust protection measure. The theory is significant since it can help organizations protect their platforms especially when multiple users have access to the system on a regular basis. IT experts can learn from the theory and gain better understanding in how to develop and design an efficient mechanism that can heighten the knowledge held by users towards technological threats. Moreover, it becomes possible for technology platform users in an organization to react actively or passively to particular threats. Improved awareness by employees regarding technology threats aids in adoption and motivation of IT platforms without adverse outcomes. Carpenter et al., (2019) asserts that IT threat avoidance is depicted in the form of cybernetic processes where the main goal is spreading distance that is between the existing information privacy concern and the possible unsafe results. Most information technology experts and users accept that reducing the prevailing threat is a more desirable coping mechanism for reduction of the threat.

2.2.2 Unified Theory of Acceptance and Use of Technology (UTAUT)

The UTAUT model is a theoretical advancement over previous theories that seek to explain adoption of information technology among different users. Venkatesh et al. (2003) proposed the model following a comprehensive review of eight different theories that were previously used to explain user behaviour. The theories reviewed include technology acceptance model (TAM), theory of reasoned action, motivational model, innovation diffusion theory, model of PC utilization, theory of planned behaviour, social cognitive theory and combined theory of planned behaviour/technology acceptance model. The aim of the researchers was to eliminate redundancy in the models arising from repetitions.

Unified Theory of Acceptance and Use of Technology (UTAUT) model helps explain the adoption and further diffusion of Information Systems by exploring user's intentions in regards to using information systems and their behaviour. Previous models on technology adoption could only account for 54% of user behavior (Williams et al., 2015). Subsequently, Venkatesh et al. (2003) conducted a comprehensive

longitudinal study with three specific data collection stages namely immediately one completed technology training, one month after training and two-months after the technology training. The researchers used a data collection instrument with 32 constructs drawn from previous models coupled with four moderators. The four moderators included age, experience, voluntariness and gender.

Following a review of the 32 constructs, the researchers came up with a simple instrument capable of explaining 70% of the IT user behavioural intentions (Venkatesh, 2003). Under the model, the difference in IT user's intentions can be measured through four constructs including effort expectancy, performance expectancy, facilitating conditions and social influence. Similarly, there are four moderating variables of gender, age, voluntariness and experience. Moreover, use behaviour and behavioural intention serve as criterion variables. Consequently, the research by Venkatesh et al. (2003) established that the predictors of effort expectancy, social influence, and performance expectancy are directly correlated with the behavioural intention of IT users. On the other hand, the facilitating conditions were identified as having a direct contribution to the actual usage of information systems. The theory is relevant to the study as it helps explain the use and growth of BYOD within organizations.

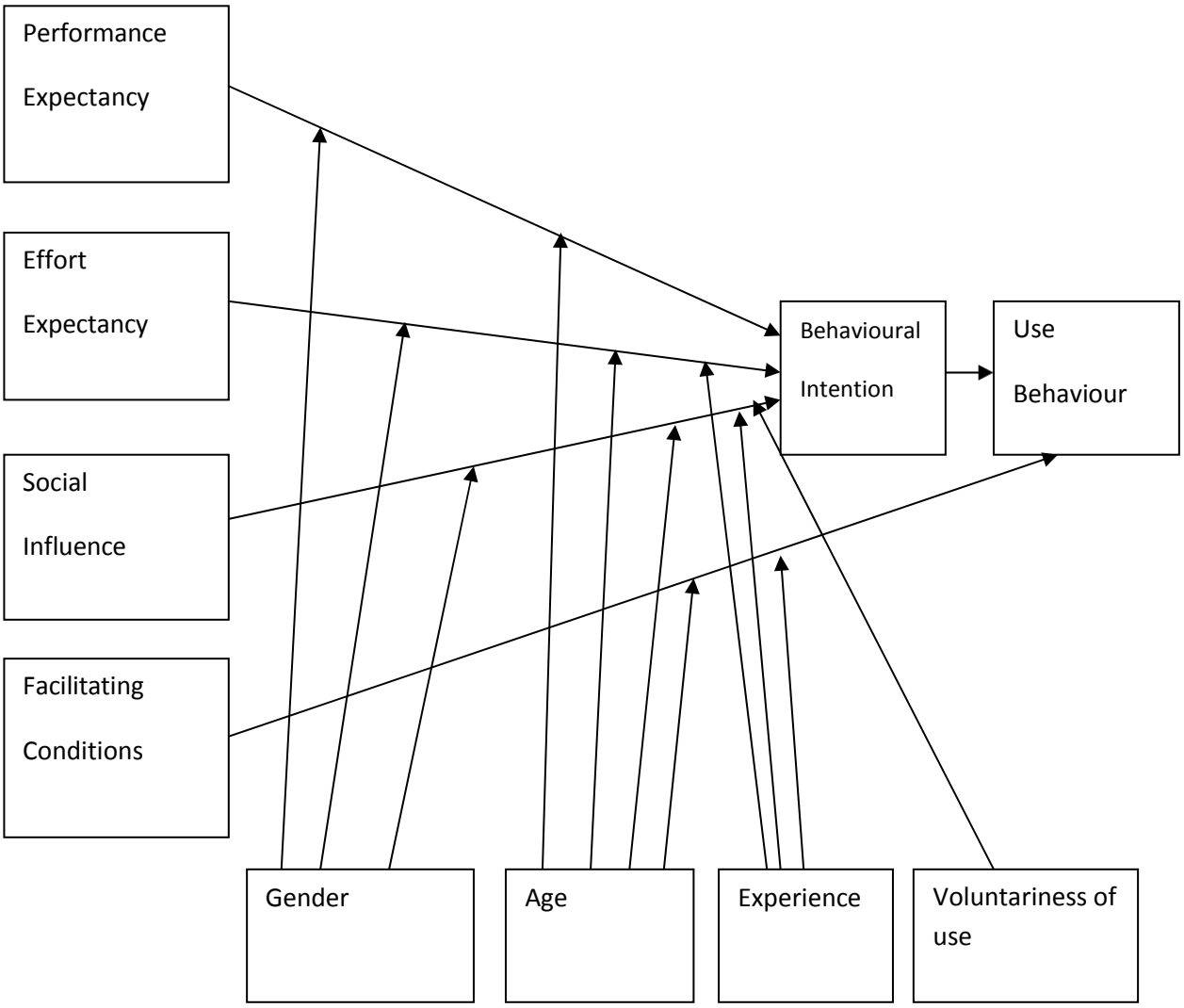


Fig 2.1: Illustration of the Unified Theory of Acceptance and Use of Technology.

Chao, (2019) asserts that Unified Theory of Acceptance and Use of Technology (UTAUT) model has been used and applied and further tested extensively for the prediction of system usage. Moreover, the theory has been used in ensuring technology adoption and technology usage decisions in varying fields including whiteboards. Other areas where the theory has been applied include the use of near-field communication technology, healthcare management, Enterprise resource planning and in telehealth services. According to Chao (2019) Unified Theory of Acceptance and Use of Technology (UTAUT) has been used in applied research with remarkable results. Moreover, Unified Theory of Acceptance and Use of Technology (UTAUT)

model provides a framework that helps explain acceptance of information technology. In addition, Unified Theory of Acceptance and Use of Technology (UTAUT) is integral to determining the acceptance and usage of technology by different users.

2.2.3 Machine Learning Techniques and Models

Machine learning models allow information systems to learn from previous experience. Subsequently, machine learning considers the system's ability to obtain and further integrate knowledge using observations and improving through learning new knowledge rather than having to be programmed beforehand for the same. Consequently, machine learning concerns multidisciplinary areas and produces statistical and computational theories for learning processes. Machine learning algorithms are used regularly in the contemporary society in different commercial systems. Consequently, machine learning techniques are able to organize the existing knowledge and further collect more knowledge by recording and further reasoning about the new data. Besides learning systems have been able to attain a myriad of results that range from basic memorization to the establishment of modern scientific theories. Machine learning systems can self-improve continuously to enable systems become more effective and efficient.

Machine learning algorithms using predictive modelling have been developed to predict future outcomes by drawing insightful conclusions from available data in an automated and structured fashion. According to Yim (2020), predictive modeling is the general notion of building a model that is capable of making predictions. Such a model typically includes a machine learning algorithm that studies certain properties from a training dataset in order to make those predictions. Machine learning algorithms basically build models of behaviors and use those models as a basis for making future predictions based on new input data. Predictive models are grouped into two, Classification models, whose task is to assign discrete class labels to certain observations as results of a prediction, and Regression models which are based on trends and the relationships analysis between variables in order to make continuous variables predictions. These

models are then made up of algorithms that perform the data mining and statistical analysis, determining trends and patterns in data. The most widely used predictive models are decision trees, regression (linear and nonlinear) and neural networks.

Today's increase of remote workers combined with flexible digital resources, opens a multitude of entry points for hackers to be able to access corporate networks. For this reason, endpoint security is a vital piece of network security in a security strategy of every corporate. Endpoint Security is the approach that organizations take to protect their network when accessed by endpoint devices such as laptops, smartphones, desktops and mobile devices. Information security is a major concern for corporations that have adopted the BYOD concept since the malware threats are created daily by individuals with bad intentions (Bilal et al., 2018). Security threats that are experienced currently attack endpoint security targeting both personal and business computer devices and this puts company data at a serious risk of being stolen or lost and this can have deleterious effects of the organization. The available protection measures include antivirus programs that work hand in hand with the security features present in computers.

Effectiveness of most antivirus programs is limited as they work by looking for particular file signatures that have a history of containing a malicious code. On the other hand, attackers keep developing new malicious programs, and also infect computer devices using unsecured wifi networks or by using seemingly harmless files that need to be downloaded. Machine learning endpoint security helps in finding uncommon patterns in user behavior to identify potential malware attacks. Machine learning offers a more reliable method for managing the challenges of malicious code in computer devices (Sarker et al., 2020).

One example of a machine learning program under use is the zIPS (Zimperium Intrusion Prevention System) technology that is able to learn how the computer device is normally used (Yim, 2020). The machine learning program learns how one uses their device and it can detect irregular behaviour before sending a notification of the problem to the user (Bilal et al., 2018). The machine learning approach under

zIPS enables future attacks to be stopped without having to know what type of attack manifested. zIPS machine learning program is superior to antivirus programs that rely on the history of malicious attacks since it does not require to encounter the malware for it to offer protection. Moreover, zIPS program is able to monitor processes taking place outside of its sandbox and this makes it dynamic and independent of particular signatures.

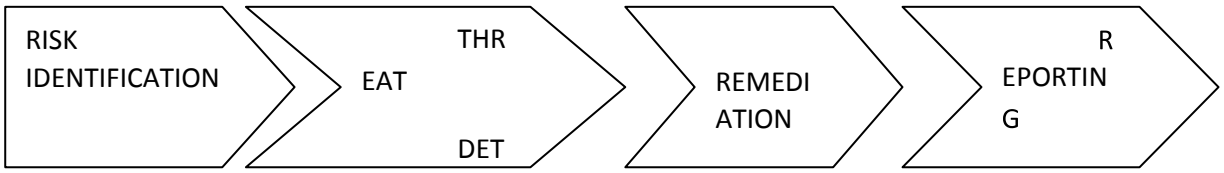


Fig 2.2: zIPS Fundamental Design Model

BYOD systems usually operate under cloud computing and its security is a major concern for organizations. Cloud computing offers flexibility in the workplace but creates more avenues for malware attacks. Machine learning technology prevents attacks by creating algorithms that can assess risks associated with the use of particular apps and identifies variations from the normal use. Consequently, machine learning will create a better platform for the integration of BYOD since it offers better protection compared to antivirus programs (Jang-Jaccard & Nepal, 2014). Cyber security measures are integral in the management of malware including viruses, bot executables, worms and Trojan horses.

Cuevas et al., (2015) proposes the Multi-platform Usable Endpoint Security System (MUSES) program that interacts with BYOD devices regardless of whether they are corporate or self-owned. The program runs in the background and monitors the interactions of the user and context of the computer use environment. The application contains two modules which include a controller and actuator. Controller element consists of several implemented sensors within the device that monitor the user's behavior and the environment. Subsequently, the actions of the user coupled with device configuration are translated into a particular sequence of events. The events generated are processed in real time using a Risk and

Trust Analysis Engine together with an Event Correlation Module (Cuevas et al., 2015). Based on the output of the Risk and Trust Analysis Engine, the corporate security officers make a decision based on the security rules applicable to the user.

On the other hand, Zainab et al., (2017) proposes a new conceptual model that is based on the modified fuzzy-Analytic Hierarchy Process that is utilized in finding the weight of the chosen criterion and sub-criterion. The two main criteria explored by Zainab et al., (2017) include 'intention in the use of technology and 'Policy-specific' criteria. The two criterions have each five sub-criteria for analysis. The sub-criterion for 'behavioral intention of using technology' include tangible results using technology, relation to work, management support, technical support and technical complexity. On the other hand, the sub-criterion for policy-specific criteria include: acceptable usability policy, device policy and support, device policy and free payment, information security policies and information access, and risk-responsibility for device policy.

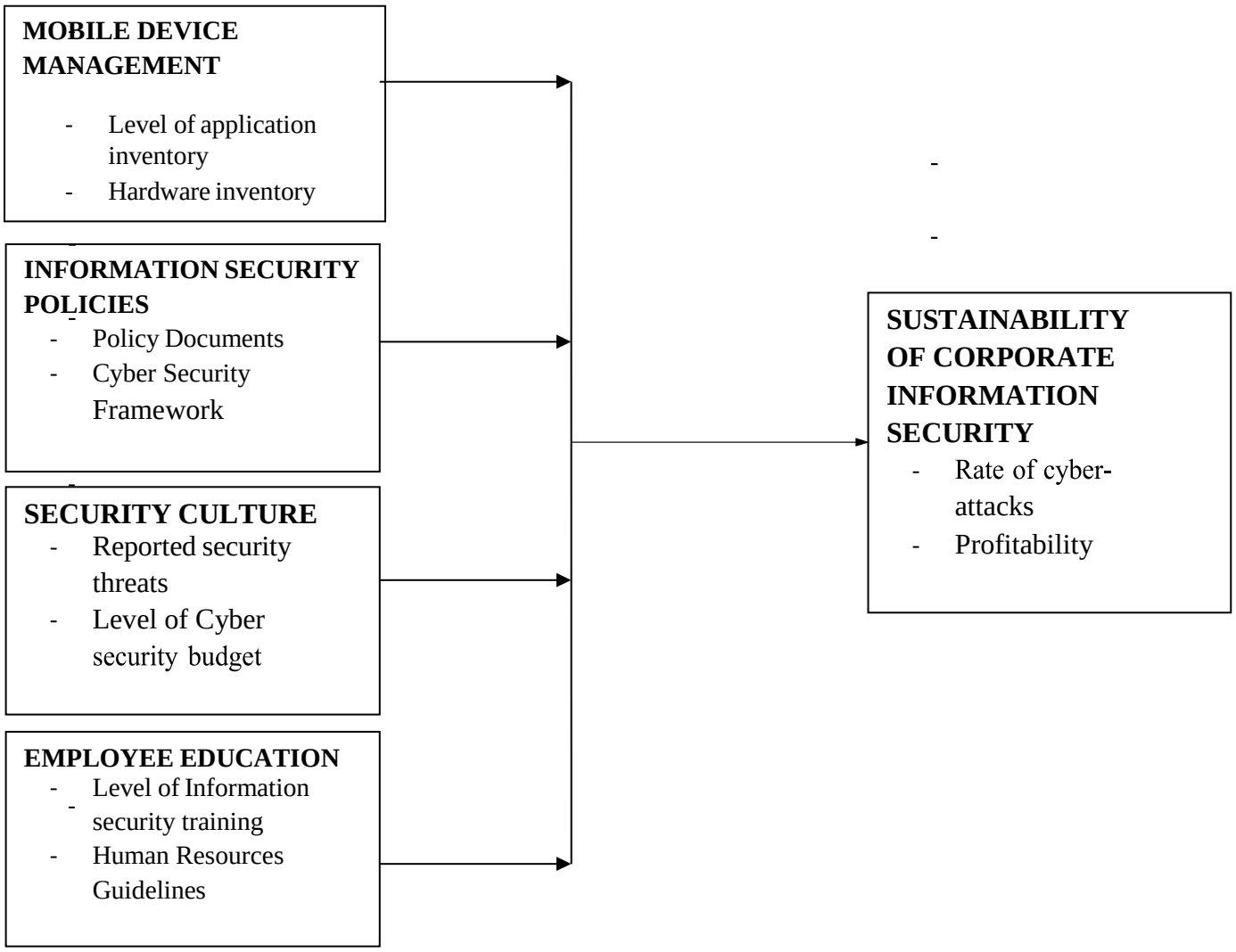
In order to create an Artificial Intelligence model, one has to avail training data coupled with evaluation data. Moreover, it is imperative that one defines the defined expiration time for the machine learning model. Besides, the quality of each model developed is dependent on the machine learning metric values. The precision for the model should exceed 0.5 while the recall should be 1 or nearby. The production of artificial intelligence models requires one to collect and further train the machine learning algorithms for the different input metric such as a soft keyboard. Once this is completed trained models are incorporated into the framework. Machine learning algorithms can use raw data points in determining the impact of novel and unseen data samples instead of developing a unique model for training and testing data (Cuevas et al., 2015). In this regard, machine learning models recognize interpretation of the available data from the features presented together with dimensions and the data point. Machine learning uses similarity measure for new data point to identify the closest input data points to the new input data point. Machine learning can use input data points and through similarity

predict new data points.

The challenges with machine learning exist and these include inability to understand patterns related to human learning. AI systems cannot provide mathematical description for human reasoning and ability for problem solving. Machine learning cannot generate cognitive models that hold a form of human capability. On the other hand, machine learning models are integral to supporting the work of human beings in different fields.

2.4 Conceptual Framework

A conceptual framework as illustrated below shows the perceived relationship between independent variables and the dependent variable. It is hypothesized that the independent variables are related to growth of the corporate information security; a proposition that partly guides the study.



Independent Variables Dependent Variable

Fig 2.3: Conceptual Framework for the Study.

2.5 Existing Research Gaps

The research undertaken previously by scholars has centred on BYOD integration in different organizations including schools, universities and business entities (Veljkovic, & Budree, 2019; Olalere et.al, 2015; McLean, 2016). Moreover, the analysis has focused on the use of mundane cyber security measures to manage information security. The researchers have failed to capture the events in banking institutions where information security is an existential threat to the institutions. Besides, the researchers undertook their studies before the advent of Covid-19 pandemic which has forced employees in different organizations to operate virtually using computer devices. Subsequently, there is a research gap in regards to the use of machine learning models in the process of information security for banking institutions. The current research study will seek to fill the research gap and provide more knowledge in regards to BYOD and corporate information security measures.

2.6 Conclusion

The current chapter has explored the different theoretical models that are applicable to the integration of BYOD in different organizations. Subsequently, the theories explored include Unified Theory of Acceptance and Use of Technology, Technology Threat Acceptance Theory and Machine learning models. In addition the chapter has illustrated the conceptual framework for the BYOD model. Moreover, the chapter has presented relevant information presented by different authors regarding risks, benefits and mitigation measures employed for the purpose of integrating the BYOD system in organizations.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

The current segment of the research study explores the procedure used in coming up with relevant data and information for attaining the study objectives. Subsequently, the chapter presents the research design, target population, sampling procedure, collection of data and analysis. The research methodology chapter assisted in gathering data for realization of set objectives. The study specific objectives included; to review the corporate information security challenges arising from the integration of BYOD in the banking sector, to examine the factors of BYOD integration that promotes a sustainable corporate information security, to design and develop the BYOD model and finallyto test and validate the model.

3.2 Research Design

The study employed a cross-sectional survey design to collect data relevant for making a conclusion on the study objectives. According to Lavrakas, (2019) cross-sectional survey is used when collecting data to help come up with inferences on a particular population at a particular point in time. Subsequently, cross-sectional surveys can be viewed as snapshots of the target population where data is gathered. The use of cross-sectional survey design helps generate quantitative data that will be analysed with a view of generating information on BYOD integration in the Kenyan banking sector. Cross-sectional surveys can be repeated periodically; however, in such situations respondents who participate in the first sampling are intentionally ignored (Payne & Payne, 2004). There are multiple benefits associated with undertaking a cross-sectional survey design including the fact that it is inexpensive. Furthermore, the research design does not need a lot of time to undertake. Other benefits include the fact that it captures data from a particular point in time. In this regard, there is clear evidence to support the use of cross-sectional survey design in examining the integration of BYOD.

3.3 Target Population

Whenever a research is undertaken, one must identify the individuals on whom the results will be generalised (Jha, 2014). Subsequently, the population of the study comprises of the individuals with the desired shared qualities that inform the study. The target population that will be studied in the current research comprises of individuals from the Kenyan banking sector. Some of the shared qualities in such a population is the fact that respondents are employees working in banking organizations operating in Kenya. The population of banking employees and stakeholders serves as the basis for the current study. Consequently, the information gathered during this study from the sample will be generalised to the target population of employees within the Kenya banking sector. The target population of employees within the Kenya banking sector will formbasis for external validity of the study. Information gathered from the banking employees regarding the use of BYOD will be generalised to the entire banking sector.

3.4 Sampling and Sampling Procedure

Once the target population is identified the next step is to select a pool of respondents that will participate in the study. It is impossible for the researcher to collect data from all the individuals within the banking sector due to the cost of such an event. Sampling is important since it will allow the researcher to focus on a particular subset of the target population (Daniel, 2012). The current study will use random sampling to determine the participants of the study.

3.4.1 Sampling Frame

The sample frame outlines the members of the target population within the study. In the current study the sampling frame captures the employees of Equity bank operating in Mombasa. The total number of Equity bank staff members within Mombasa County stands at 1080.

Table 3.1: Target Sample Population

Description	Population in Numbers
Management Staff	195
Junior-level Staff	885
Total	1080

3.4.2 Sample Size Determination

The exact sample size was determined using the Nassiuma's Formula as presented below:

$$n = \frac{NC^2}{C^2 + (N - 1)\, e^2}$$

Where: n=sample size

N=Population

C= coefficient of variation ($21\% \leq C \leq 30\%$),

e= the precision level ($2\% \leq e \leq 5\%$)

The formula was used to calculate the sample as shown

$$n = \frac{1080 \times 0.25^2}{0.25^2 + (1080 - 1)\, 0.03^2}$$

$n = 65.30$

$n = 65$ respondents

3.5 Research Instrument

The study utilized a questionnaire with the view of obtaining relevant data consistent with the study objectives. Questionnaires serve as the best and appropriate tools for the collection of primary data while undertaking survey studies within a large population of respondents (Byrnes, 2009). The study used close ended questionnaires consisting of Likert scale in order to generate quantitative data.

3.6 Pilot Testing

In order to determine the validity and reliability of the questionnaire, the study was taken through a comprehensive pilot test. The pilot test was undertaken on a few bank employees within Mombasa County .Baker (1994) asserts that a pilot study entails the pre-testing of the research instrument; in this case a questionnaire, with the intention of heightening efficiency of the entire process. A sample size of 10-20% of respondents from the target population was sufficient for the pilot test. Subsequently, the current study used a sample of 8 respondents from the banking sector to run the pilot test.

3.6.1 Validity Test

A research instrument should be able to accurately measure the intended objects and provide the correct information (Daniel, 2012). Content validity of the research instrument was established through the use of Kaiser-Meyer-Olkin (KMO) and Bartlett's Test of Sphericity consultation with research experts. KMO test indicates the fraction of variance in the variables caused by the underlying factors. A value close to 1.0 is desirable. On the other hand, Bartlett's test of Sphericity helps determine whether factor analysis can be sufficient with the data. Table 3.1 shows that KMO value exceeds 0.5 implying that the sample is sufficient for factor analysis. Moreover, the Bartlett's Test of Sphericity indicates a value less than 0.05 of significance level. The results show that the research instrument used in data collection had content validity.

Table 3.2: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy	.733	
Bartlett's Test of Sphericity	Approx. Chi-Square	67.723
	df	6
	Sig.	<.001

3.6.2 Reliability Test

The reliability test is integral in determining the internal consistency of the research instrument (Scott, 2019). Subsequently, the study used the Cronbach Alpha test to determine the internal consistency. It was imperative that a questionnaire produced consistent results once administered on different samples drawn from the same target population. A questionnaire that passes the reliability test should have a value greater than 0.7. On the other hand, a value below 0.7 indicates that the questionnaire needs to be improved.

Table 3.2: Reliability Analysis

Variable	Test Items	Alpha Values
Mobile Device Management	4	0.756
Information Security Policies	4	0.738
Security Culture	4	0.766
Employee Education	4	0.788

A comprehensive pilot study was undertaken with a view of determining the reliability of the questionnaire. Using the Cronbach Alpha metric, the internal consistency of the questionnaire was determined and it established that the four study variables questions were reliable. According to table 3.2, Mobile Device Management had a reliability of 0.756; Information Security Policies 0.738; Security Culture had 0.766 and Employee Education 0.788. Since the study variables had alpha values exceeding 0.7, the questionnaire was deemed as reliable.

3.7 Data Collection Procedure

Once the pilot test was complete, the required correction was undertaken, and a consent for data collection sought from the authorities. A formal letter of introduction from KCA University was obtained and served to introduce the researcher to the target population. Similarly, a letter of consent from Equity bank management was sought to ensure that the researcher has authority to access the respondents in their

places of work. The questionnaires were administered through the human resources management in the different bank branches in the month of May 2021. Following the administering of the questionnaires, I followed up on the progress of filling the data collection instrument on a weekly basis. Finally, in early June 2021 the questionnaires were collected from the same human resources department after a period of three weeks had elapsed. The questionnaires collected were in a good state and clean hence ensuring that data recording and input was correct.

3.8 Data Processing and Analysis

The quantitative data was analysed in order to come up with findings and conclusion. Once the questionnaires were returned, the researcher utilized the Statistical Package for Social Sciences (SPSS v27) to analyse the data. The data was analysed using inferential statistics. The inferential statistics included correlation statistics and multiple regressions analysis. Multiple regressions is an example of ordinary least-squares model since it entails multiple explanatory variables. The multiple regressions function used in the study is illustrated below:

$Y= \beta 0 + \beta 1X1+ \beta 2X2+ \beta 3X3+ \beta 4X4 +\varepsilon$ Where:

Y	=	Sustainable Corporate Information security
$\beta 0$	=	Constant
X1	=	Mobile device management
X2	=	Information Security Policies
X3	=	Security Culture
X4	=	Employee Education
ε	=	ErrorTerm

$\beta 1, \beta 2, \beta 3, \beta 4$ = Regressions Coefficients

3.8.1 Ethical Considerations

The research process was guided by ethical guidelines including informed consent, and respect for respondents confidentiality. Moreover, the research respected the privacy of the respondents and the organizations they represented. In this regard, the data collection process involved unmarked questionnaires that did not indicate the respondent's personal details.

CHAPTER FOUR

DATA ANALYSIS, FINDINGS AND DISCUSSIONS

4.1 Introduction

The following chapter of the research commences with an illustrative description of the findings drawn from collection of data. The data was collected from 60 respondents who represent 92.3% of the sample population. Subsequently, within this chapter, data is presented through the form of distribution tables that aid in the description of findings coupled with the relevant explanation. The discussion of findings was meant to attain the specific objectives set for the study.

The study specific objectives included; to review the corporate information security challenges arising from the integration of BYOD in the banking sector, to examine the factors of BYOD integration that promotes a sustainable corporate information security, to design and develop the BYOD model and finally to test and validate the model.

4.2 Response Rate for the Study

Table 4.1: Response Rate

	Questionnaires Administered	**Questionnaires filled & Returned**	**Percentage**
Respondents	65	60	92.3 %

The researcher sought to gather data from stakeholders within the Kenya Banking Sector and more specifically within Equity Bank. Subsequently, a response rate of 92.3% was achieved and this is satisfactory for generalization of the findings.

4.3 Demographic Information

4.3.1 Gender Distribution

Table 4.2: Distribution of Respondents by Gender Category

	Frequency	Percentage
Male	26	43.3
Female	34	56.7
Total	**60**	**100.0**

The findings illustrated on table 4.3 indicate that a majority of the respondents were female at 56.7%. On the other hand, 43.3% of the respondents were male. Subsequently, a majority of employees in the Kenyan banking sector are female.

4.3.2 Length of Service in the Organization

Table 4.3: Length of Service

	Frequency	Percentage
0-5Years	30	50.0
6-10 Years	20	33.3
11-15 Years	6	10.0
Above 16 Years	4	6.7
Total	**60**	**100.0**

According to table 4.4 a majority of the respondents have worked in the banking sector for less than five years (50%). The second most populous group of respondents are those who have worked for between 6-10 years in the bank (33.3%). Similarly, respondents who have worked for 11-15 years are 10% of the entire population and 6.7% for those who have worked for above 16 years.

4.3.3 Age Category

Table 4.4: Spread of Respondents by Age

	Frequency	Percentage
Below 25 Years	5	8.3
26 - 35 Years	41	68.3

35-45 Years	11	18.3
Above 45 Years	3	5.0
Total	**60**	**100.0**

According to table 4.5, a majority of the respondents (68.3%) are between the age of 26 and 35 years old. Similarly, 18.3% of the respondents are between 35 and 45 years old; those below 25 years make up 8.3% of the population. Finally, the minority population is that of respondents above 45 years of age at 5%.

4.3.4 Level of Education

Table 4.5: Level of Education

	Frequency	**Percentage**
College Diploma	5	8.3
Degree	40	66.7
Postgraduate	15	25.0
Total	**60**	**100.0**

Table 4.6 shows that a majority of the respondents in the banking sector have a first degree qualification at 66.7% of the population. The second most populous category is postgraduate at 25% of the respondents. Finally, 8.3% of the respondents have a college diploma.

4.4 Research Findings

4.4.1 Objective One Results

The first objective of the research study was to review the corporate information security challenges arising from the integration of BYOD in the banking sector. Subsequently, the research established from the respondents through the questionnaire that the following are the main challenges:

i. Management and control of the BYOD platform

This challenge was established from part B in the questionnaire. From table 4.7, we can see 38 respondents and 22 respondents strongly agree and agree respectively, to the fact that mobile device management is

essential in security of corporate information.

Table 4.6: Mobile Device Management

Mobile device management tools are essential to ensuring enterprise compliance in relation to users privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	38	63.3	63.3	63.3
	Agree	22	36.7	36.7	100.0
	Total	60	100.0	100.0	

ii. Limited knowledge of novel technological threats by the employees

From table 4.8, 17 respondents disagree and 25 respondents strongly disagree with the fact that they have sufficient knowledge regarding technological threats that threaten the security of corporate information. This is a huge number compared to the respondents who agreed to have the knowledge. As a result this challenge was noted. This data was sought from part E of the questionnaire.

Table 4.7: Employee Education

Employees in the institution have sufficient knowledge regarding sustainable corporate information security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	3	5.0	5.0	5.0
	Agree	4	6.7	6.7	11.7
	Neutral	11	18.3	18.3	30.0
	Disagree	17	28.3	28.3	58.3
	Strongly Disagree	25	41.7	41.7	100.0
	Total	60	100.0	100.0	

iii. Lack of a proper BYOD device register by organization IT department

Table 4.9 depicts a large number of respondents disagree than agree with the fact that their organization's IT department adequately manages reported computer security threats. This leads to the conclusion that

there is lack of a proper BYOD device register in the respondent's IT department. This data was collected from part D of the questionnaire and analyzed using SPSS.

Table 4.8: BYOD device register

Reported computer security threats are adequately managed by the IT department to ensure sustainable corporate information security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	9	15.0	15.0	15.0
	Agree	10	28.3	28.3	43.3
	Neutral	9	15.0	15.0	58.3
	Disagree	31	40.0	40.0	98.3
	Strongly Disagree	1	1.7	1.7	100.0
	Total	60	100.0	100.0	

iv. Financial limitations in the running and management of the BYOD platform.

Table 4.10 shows that 32 respondents out of 60, disagree and strongly disagree with the fact that the organization's financial resources dedicated to corporate information security is sufficient. This challenge needs to be addressed appropriately so as to enhance security. This data was sought from respondents through part D of the administered questionnaire.

Table 4.9: Financial limitations.

The financial resources dedicated to corporate information security is sufficient

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	1.7	1.7	1.7
	Agree	9	15.0	15.0	16.7
	Neutral	18	30.0	30.0	46.7
	Disagree	20	33.3	33.3	80.0
	Strongly Disagree	12	20.0	20.0	100.0
	Total	60	100.0	100.0	

4.4.2 Objective Two Results

The second objective of the research study was to examine the factors of BYOD integration that promotes a sustainable corporate information security. After using SPSS for analysis, the results for the second objective are illustrated in table 4.7.

Table 4.10: Results for objective two

Variable	B	Significance
(Constant)	2.401	.001
Mobile Device Management	0.055	.000
Information Security Policies	0.230	.026
Security Culture	-0.309	.004
Employee Education	0.240	.012

Subsequently, following the analysis, the researcher established that Mobile device management, Information security policies, Security culture and Employee education are statistically significant in the attainment of a Sustainable corporate information security when using BYOD within the banking sector. Moreover, the table indicates that as Mobile device management index changes by a value of 1, it leads to a change of 0.055 change in sustainable corporate information security. Similarly, if the Information security policies index changes by a value of 1, then a 0.230 change in sustainable corporate information security. Besides, an increment by a value of 1 in Employee education levels leads to a 0.24 change in the Sustainable corporate information security. On the other hand, Security culture has a negative value implying a change in the existing security culture will lead to a poorer corporate information security within the BYOD platform in the banking sector.

4.4.3 Objective Three Results

The objective was to design and develop a BYOD Model that will lead to a Sustainable Corporate Information Security within the banking sector.

$Y = \beta 0 + \beta 1X1 + \beta 2X2 + \beta 3X3 + \beta 4X4 + \varepsilon$ Where:

Y	=	Sustainable Corporate Information security
$\beta 0$	=	Constant
X1	=	Mobile device management
X2	=	Information Security Policies
X3	=	Security Culture
X4	=	Employee Education
ε	=	Error Term
$\beta 1, \beta 2, \beta 3, \beta 4$	=	Regressions Coefficients

Therefore, Sustainable Corporate Information Security= 2.401+0.055 Mobile Device Management+0.230 Information Security Policies-0.309 Security Culture+0.240 Employee Education

The developed model shows that mobile device management, information security policies, security culture and employee education have a significant association with sustainable corporate information security within the Kenya Banking Sector. Subsequently, changes in the value of the variables affect sustainable corporate information security when integrating BYOD in the banking sector.

4.4.4 Objective Four Results

The fourth objective of the research study was to test and validate the model. Subsequently, Model Summary and ANOVA were used. The researcher developed an OLS model using multiple regressions to test the impact of the predictor variables on the dependent variable. Subsequently, SPSS v27 was used to input, code, and compute multiple regressions statistics. The model summary is illustrated in table 4.8.

Table 4.11: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.690[a]	.476	.437	.421

a. Predictors: (Constant), Mobile Device Management, Information Security Policies, Security Culture, Employee Education

As illustrated in table 4.8, the correlation existing between the independent variables (Mobile Device Management, Information Security Policies, Security Culture, Employee Education) and the dependent variable of sustainable corporate information security (R=0.690). On the other hand, the Adjusted R-Square which is the coefficient of determination (r^2=0.437) indicates a 43.7% change in sustainable corporate information security under BYOD attributable to the four predictor variables. In this regard, there are a myriad of other factors affecting BYOD information security and this needs to be explored.

Table 4.12: ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	8.847	4	2.212	12.472	.001[b]
	Residual	9.753	55	.177		
	Total	18.600	59			

a. Dependent Variable: Sustainable Corporate Information Security

b. Predictors: (Constant), Mobile Device Management, Information Security Policies, Security Culture, Employee Education

On the other hand, table 4.9 depicts the Analysis of variance results which has been used in the study for the purpose of determining whether there are any statistically significant differences between the mean/average of the four independent variables. The main limitation of the ANOVA test statistic is the fact that it cannot describe which specific groups in the data set that are statistically different from each other (Hirotsu, 2017). In the current ANOVA analysis the generated significance value is 0.001 which also implies a p-value of .001 that is below 0.05. Consequently, there is a statistically significant difference

between the means of the independent variables Mobile Device Management, Information Security Policies, Security Culture, and Employee Education. The limitation of ANOVA test statistic prevents us from determining the specific variables that differed.

4.5 Discussion of Results

The research study involved 60 respondents from the Kenya banking sector who have utilized the BYOD platform in their places of work. At 5% level of significance, it was established that the four independent variables chosen – Mobile device management, Information security policies, Security culture and Employee education- had a significant effect on sustainable corporate information security.

The general objective of the research was to establish a model for BYOD integration to increase sustainable corporate information security in the Kenya banking sector. Subsequently, four aspects of BYOD were reviewed to determine their impact on sustainable corporate information security.

Subsequently, the data collection process reviewed the variables of the study and established that the management of Mobile devices used in the BYOD platform is imperative. Such findings correlate with those of Chao et al. (2020) who posit that progressive organizations have integrated BYOD in the workplace and management of the platform heightens the proper usage of devices. Moreover, Jiunn-Woei (2020) affirm the importance of Mobile device management through cloud computing technology and the use of smart devices.

Similarly, Information security policies was identified as a significant aspect of BYOD integration in the study. Such policies are meant to guide the bank employees on how to mitigate against information security threats. The study findings indicate that information security policies are integral in the management of new technological platforms such as BYOD. The findings are consistent with those by Ahmed et al. (2017) who stated that novel technology platforms are linked with privacy and security risks. Subsequently, the establishment of information security policies is critical in BYOD. On the other hand, the study established that changes in the security culture of the organization can lead to diminished corporate information security. Subsequently, the findings are inconsistent with those by Weeger et al. (2020) asserts that

organizations with younger generation employees are better at integrating BYOD. The current findings indicate that a security culture relating to BYOD can contribute towards decline in corporate information security regardless of the age demographic of users. The majority of the respondents (68.3%) were between 25 and 35 years of age which is a youthful population.

The proper integration of BYOD requires supportive policies from the organisation coupled with resource availability. Many organisations globally are making considerable progress towards successful integration of BYOD. Organisations are increasingly providing the latest mobile and IT devices that enable employee's access the resources of the company (Chao et al., 2020). The main objective of integrating BYOD into the organisation is to improve the level of employee satisfaction and their performance through flexibility in the workplace. On a different note, the continuous growth and integration of BYOD has led experts to review the corporate security measures associated with privacy and company documents. Concerns arise from the ability of employees to move with company information to their homes coupled with remote access to sensitive documents.

Conversely, the research established that employee education was significant in developing a sustainable corporate information security under BYOD. The results are consistent with the Technology threat avoidance theory as presented by Liang and Xue (2009). The theory provides that once technology users perceive a threat, they will become motivated to overcome and avoid the threat. Subsequently, users who perceive computer information security threats are more likely to accept education and training for BYOD use hence improving the corporate information security. Employee training and education heightens the knowledge held by the respondents when using their personal devices to access company information technology platform.

4.6 Summary

Following the comprehensive data analysis the study established that the four independent variables of Mobile device management, Information security policies, and Security culture and employee education

have a significant effect on the corporate information security. Subsequently, integration of BYOD in the banking sector requires to be guided the following OLS model: Sustainable Corporate Information Security= 2.401+0.055 Mobile Device Management+0.230 Information Security Policies-0.309 Security Culture+0.240 Employee Education.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The following section explores the conclusions derived from the model developed during the data collection and analysis of information from the Kenya banking sector. Furthermore, contribution of the study and recommendations by the researcher will be provided in this chapter.

5.2 Conclusions

The respondents drawn from the banking sector were of the view that a robust mobile device management system is essential for a sustainable corporate information security when BYOD was being used. A mobile device management system will bring on board all devices used through BYOD and have them linked with the organization ICT Security system. The study established that an inventory of all devices under BYOD should be managed by the developed organization information security system. Moreover, through multiple regressions it is clear Mobile device management has a positive relationship with sustainable corporate information security while using BYOD in the banking sector. Subsequently, banking organisations in Kenya should dedicate more financial resources to their IT departments which are responsible for Mobile device management. A functional BYOD platform requires transparency in the devices used and this implies that IT departments require to use mobile device management tools to ensure employees devices do not lead to computer threats.

On the other hand, the respondents felt that information security policies were not clearly articulated when one considered BYOD use in the Kenya banking sector. Most organizations have not documented clearly the information security policies that guide BYOD use. Documentation of policies is vital in any organization as it ensures stakeholders have guidelines for particular situations they may find themselves in during implementation of their roles. Clear illustration of information security policies is preferred by

the bank employees who use their personal devices to undertake work. Moreover, the research established that having a cyber-security framework augments the corporate information security.

Respondents felt that the existing security culture was instrumental in how arising issues were addressed by the IT department. Moreover, the respondents admitted that computer security threats are numerous but the security culture aided in reporting and subsequent reaction. It was not clear whether financial resources were adequately provided to the IT department to heighten security of the information technology. Such a finding can be attributed the top-down management system and information flow as most of the respondents were junior level employees lacking managerial information privilege. Besides, the respondent sought to have an improved security culture in regards to the use of BYOD within their organization.

Employee education on corporate information security significance in BYOD was identified as being essential for a sustainable corporate information security. The respondents were of the opinion that training was important in developing a sustainable corporate information security while using BYOD in the bank. Employee training and education heightens the knowledge held by the respondents when using their personal devices to access company information technology platform. Moreover, employees were receptive to the idea of training on sustainable corporate information security while using BYOD. Subsequently, training resources for such activities can heighten the level of Corporate information security in the banking sector.

BYOD adoption has been found to be especially beneficial since it improves the technology knowledge and acceptance within the organization which is essential for a motivated workforce. Moreover, the adoption of BYOD in institutions is favored by heightened efficiency and ability to learn different aspects relevant to organizational tasks. Besides, using standard organizational devices ensures that employees and stakeholders in the organization are able to undergo a smooth learning curve. Employees with hectic schedules and deadlines can benefit from using familiar standard devices under the BYOD

system hence improving the amount of time and energy one can put on the main task. Moreover, the features of potential adopters, innovation available and local context determine the level of technology adoption within the organization. BYOD integration improves when the individuals involved are innovative and with a high rate of computer self-efficacy. It is imperative that the users and other stakeholders of the BYOD platform are trained on its use regularly. Besides, superior innovations and personal devices that are user-friendly and compatible with daily tasks will help improve BYOD adoption in banks and other institutions.

The constant growth of technology adoption in Kenya coupled with a population where the youth are the majority is integral to the adoption and use of BYOD. Subsequently, the young generation that now works in different organizations has brought mobile devices to the workplace. Organizations in the contemporary Kenyan society have integrated technology and connectivity to capture the benefits associated with use of information technology. Top management in different Kenyan organizations have seen the need to utilize technology in the daily operations of the workforce and further ensured that employees can use personal devices. Subsequently, the adoption of BYOD in different organizations including banks continues to heighten and this helps improve productivity. Organizations in Kenya have adopted BYOD because it offers improved productivity and efficiency in the workplace. Similarly, organizations have realized that BYOD offers much needed flexibility at the workplace unlike the traditional working hours. Moreover, the use of BYOD is associated with heightened employee morale.

5.3 Contributions of the Study

The use of BYOD in the banking sector is more pronounced as most banks have digitized their entire operations. Subsequently, employees find the use of their personal devices to access company information as vital and convenient for their operations. The current study adds knowledge regarding the implementation of Multi-platform Usable Endpoint Security System as proposed by Cuevas et al. (2015). The program runs in the background and monitors the different devices in the BYOD platform.

Subsequently, the findings of this research augment the need for improved mobile device management using programs such as MUSES. It is imperative to gather knowledge on how best to employ BYOD policy while protecting the company information. The sentiments gathered by this research is mostly from the junior employees who are the most populous demographic within the banking sector. Subsequently, the knowledge will aid top management in better decision making regarding the use of BYOD. Security threats will continue to evolve and it thus essential to use available resources to gather knowledge on how best to retain BYOD use within organizations in the digital era.

BYOD is a reliable information system and strategy that corporations can use to generate maximum benefits. The platform is a technical innovation that Banking institutions and information technology corporations can use to streamline business operations and processes. The information generated by this research can help guide corporations such as CISCO and IBM which are leading technology companies come up with better technical solutions appropriate for running daily operations and tasks of different companies beyond the financial sector. Such technical solutions can be developed with a keen eye on how to mitigate the different risks associated with BYOD integration. Some of the threats reviewed and identified during the research include: Advanced Persistent Threat (ATP), Operating system fragmentation, false security certificates, Social engineering and Application Store.

Furthermore, this research contributes sufficient knowledge to show that every security model developed for BYOD is unique to that platform. Subsequently, there is no single information security framework that can sort the challenges posed in every BYOD framework. Since there is no integral security system that can aid in avoiding all the threats, it is imperative that information technology professionals customize their security solutions to the needs of the organization. The basic controls that should guide every BYOD model include organization policy controls, user authentication passwords, and employee profiles, encryption of hardware devices and use of GPS lock. The policies enacted by organizations should be robust enough to manage the different challenges that arise during daily

operations. Subsequently, this research reminds the organizational management and IT department that, information security policies and regulations should be updated regularly. Moreover, such policies and regulations should not be developed based on traditional corporate owned technology devices. The entry of personal devices in organizations will continue to increase and it is imperative that information security policies and framework correlates with the emerging needs.

5.4 Recommendations for Future Research

The growth of information technology use necessitates a situation where employees have to use their personal devices to access company information. It is imperative that such access is secure, convenient to the employee and well managed system by the bank IT department. The IT department should develop a robust mobile device management system that monitors all devices accessing company platform. Moreover, the banking sector players should allocate financial resources to the BYOD segment as it affects the sustainable corporate information security of the organization. On the other hand, future research should be undertaken to review the effects of top management support on the implementation of BYOD systems in the organizations. Such a research will provide guidance to management on their unique role in the development of robust BYOD systems and integration into the organization.

Banks should ensure that the information security policies developed for BYOD are well documented and made available to the employees in the organization. Subsequently, the BYOD framework recommended by the researcher is one that lays focus on mobile device management system, enhanced security culture and employee training on safe use of BYOD. It is imperative that future research explores the novel BYOD solutions offered in the market. The personal devices brought by employees keep changing and exploring their strength and weakness is vital. Similarly, it is important for future research to explore organizational controls established for the purpose of managing risks within the BYOD platform. The organizational control policies on BYOD differ and have varying success in managing risk. Consequently, research should be undertaken based on the different industries.

REFERENCES

Ahmad, M.L. (2015). Unified Theory of Acceptance and Use of Technology (UTAUT): A Decade of Validation and Development.

Ahmed, E. , I.Yaqoob, I. A. T.Hashem, I.Khan, A. I. A.Ahmed, M.Imran, A. V.Vasilakos et al. (2017). The Role of Big Data Analytics in Internet of Things. *Computer Networks* 129 (24): 459–471. DOI:10.1016/j.comnet.2017.06.013.

Arpaci, I. (2015). A Qualitative Study on the Adoption of BYOD Practice. *International Journal of E-Adoption, 7* (2).

Barlette, Y., Jaouen, A., & Baillette, P. (2021). Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers' coping strategies. *International journal of information management*, *56*, 102212. https://doi.org/10.1016/j.ijinfomgt.2020.102212

Bilal A., Wang J., Zain A. A. (2018). Role of Machine Learning and Data Mining in Internet Security: Standing State with Future Directions. *Journal of Computer Networks and Communications*, Article ID 6383145. https://doi.org/10.1155/2018/6383145

Boysen, S., Hewitt, B., Gibbs, D., & McLeod, A. (2019). Refining the Threat Calculus of Technology Threat Avoidance Theory. *Communications of the Association for Information Systems*, *45*. https://doi.org/10.17705/1CAIS.04505

Byrnes, M. E. (2009). *Field sampling methods for remedial investigations*. Boca Raton: CRC Press.

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining Technology Threat Avoidance Theory. Communications of the Association for Information Systems, 44, pp-pp. https://doi.org/10.17705/1CAIS.04422

Chao, K.-M., Jiang, L., Hussain, O. K., Ma, S., & Fei, X. (2020). *Advances in e-business*

engineering for ubiquitous computing: Proceedings of the 16th International Conference on e-Business Engineering (ICEBE 2019).

Chao, C. (2019). Factors determining the behavioural intention to use mobile learning: An application and extension of the UTAUT model. Frontiers in Psychology, 10 (1).

Chalee V., Soontorn S., Ekkachan R., & Visut S. (2017). A Policy-Based Framework for PreservingConfidentiality in BYOD Environments: A Review of Information Security
Perspectives. *Security and Communication Networks,*
Vol. 2017. https://doi.org/10.1155/2017/2057260

Cuevas et al. (2015). Corporate Security Solutions for BYOD: A Novel User-Centric and Self-Adaptive System. Computer Communications.

Daniel, J. (2012). *Sampling essentials: Practical guidelines for making sampling choices*. Los Angeles: Sage.

Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in psychology*, *9* (744). https://doi.org/10.3389/fpsyg.2018.00744

Frits G.J.J., et al (2018). Management Information System for Monitoring and Inspection of the Implementation of Universities, 7 (2.13), pp.451-456.

Jang-Jaccard, J., & Nepal, S. (2014). A Survey of emerging threats in cyber security. *Journal of Computer and System Sciences, 80* (5), pp. 973-993.

Jamal, F., Taufik, M.A., Abdullah, A., & Mohd, Z. H. (2019). A systematic review of BYOD Authentication Technique. Journal of Physics: Conference Series.

Jha, A. S. (2014). *Social research methods*. New Delhi: McGraw Hill Education (India).

Jiunn-Woei L. (2020) Understanding cloud-based BYOD information security protection behaviour in smart business: in perspective of perceived value, Enterprise Information Systems, DOI: 10.1080/17517575.2020.1791966

Lambe, I., Mary, L., & Theresa, O. (2015). A Systematic Review of Budgeting and Budgetary Control in Government Owned Organizations. *Research Journal of Finance and Accounting, 6* (6).

Liang, H., & Xue,Y.(2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly, 33* (1), pp.71-90.

Lavrakas, P. J. (2019). *Experimental methods in survey research: Techniques that combine random sampling with random assignment*.

Lawrence, C. L. (2018). Factors Affecting the Adoption of Bring Your Own Device by Teachers in Caymanian Public High Schools. *Walden Dissertations and Doctoral Studies*. 5217. https://scholarworks.waldenu.edu/dissertations/5217

Karma.N.G. (2014). Key factors affecting mobile banking adoption among bank customers in Sudan, *International Journal of Liberal arts and Social Science.* 2(*6*).

McLean K. J. (2016). The Implementation of Bring Your Own Device (BYOD) in Primary [Elementary] Schools. *Frontiers in psychology, 7*, 1739. https://doi.org/10.3389/fpsyg.2016.01739

Musarurwa, A., Flowerday, S., & Cillers, L. (2017). Individual Traits that determine the Bring Your Own Device Information Security culture: A case study of the banking sector in Zimbabwe. *Information Institute Conferences, Las Vegas*.

Laukkanen, T., (2016). Consumer adoption versus rejection decisions in seemingly similarservice innovations: The case of the Internet and mobile banking. Journal of Business Research. Vol. 69

No. 7, pp. 2432–2439.

Nalin, A.G.A., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38* (7), pp.304-312.

Olalere, M., M. T. Abdullah, R. Mahmod, and A. Abdullah. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open* 5 (2): 1–11. doi:10.1177/2158244015580372.

Palanisamy, R., Norman, A.A., & Kiah, L. (2020). BYOD Policy Compliance: Risks and Strategies in Organisations. *Journal of Computer Information Systems*.

Sarker, I.H., Kayes, A.S.M., Badsha, S. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data 7*, (41). https://doi.org/10.1186/s40537-020-00318-5

Saxena, N., et al. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. Electronics 9 (9). https://doi.org/10.3390/electronics9091460

Scott, J. J. (2019). *Learn to use Cronbach's coefficient alpha test in R with data from the British Crime Survey (Unrestricted Teaching Dataset) (2007--08).*

Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly 27*(3), pp.425–478.

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

Venkatesh, V.; Davis, F. D. (2000), "A theoretical extension of the technology acceptance model: Four longitudinal field studies", Management Science, 46 (2): 186–204, doi:10.1287/mnsc.46.2.186.11926

Wachaiyu, V.W. (2016). Monitoring and Evaluation Factors Influencing Success of Development Projects: A Case of Starehe Sub-County, Kenya. University of Nairobi, Dissertation.

Weeger, A., Wang, X., Gewald, H. et al. (2020). Determinants of Intention to Participate in Corporate BYOD-Programs: The Case of Digital Natives. Inf Syst Front 22, 203–219. https://doi.org/10.1007/s10796-018-9857-4

Williams, M.D., Rana, N.P. & Dwivedi, Y.K. (2015). The unified theory of acceptance and use of technology (UTAUT): a literature review. *Journal of Enterprise Information Management, 28*(3), pp. 443-488.

Yim, C. (2020). A New Lesson for Remote Education: Chromebooks Need More Security. *Zimperium Mobile Security Blog*. Retrieved from https://blog.zimperium.com/a-new-lesson-for-remote-education-chromebooks-need-more-security/

Zainab,A., Soomro,S., Riyaz, M.B., & Shamshirb, S. (2017). A New Conceptual Model for BYOD Organizational Adoption. *Asian Journal of Science, 10* (4), pp.400-405.

Zamhariah, B. (2018). Modelling Semantics of Security Risk Assessment for BYOD using Metamodelling Technique. *University Teknologi Malaysia*.

Zambrano, F.R.R., & Rafael, G.D.R. (2017). Bring Your Own Device (BYOD): A survey of threats and security management models. *International Journal of Electronic Business, 10* (Y).

APPENDICES

APPENDIX 1: RESEARCH SCHEDULE

The Gantt Chart presented below shows the timeline for research study.

WORK DONE	Feb-19	Sep-20	Nov-20	April-21	July-21
Identification of research topic and supervisor					
Proposal preparation					
Proposal presentation and defense					
Correction of the proposal					
Data collection					
Data cleaning					
Model Formulation					

Model Testing					
Model Validation					
Compiling presentation and defense of the Research project Report					

Table A1 : Research Schedule Gantt Chart

APPENDIX II: RESOURCES AND BUDGET

The following section illustrates the resources needed to undertake the research study.

No.	Item	Quantity	Specification	Unit Cost(Ksh)	Total Cost
1	Library Services	10 months	Subscription	500	5,000
2	Cell Phone Usage Charges	10	Safaricom Postpaid	3,000	30,000
3	Internet Expenses	10 months	Zuku Subscription	4,200	42,000
4	Statioanary	2	rims 3 pens,2 pencil,1 ruler Eraser, file, stapler,paper punch Toner	@50 0 120 380 2500	1500 120 380 2500
5	Laptop	1	Asus	60,000	60,000
6	Antivirus	2 years	Kaspersky, 1 Device		6,385.99
7	Flash Disk	1	8 gb		1500

8	Secretarial Services				5,500
9 10	Binding Printer	3 1	 Hp deskjet	1500 6000	4,500 6000
11	Travelling	6 trips	Sgr Mombasa to Nairobi Fare within the cities	3,000	18,000 5,000
12	Miscellaneous			20,000	20,000
	Total				208,386

Table B1: Resources and Budget

APPENDIX III: QUESTIONNAIRE

You are kindly requested to complete the attached questionnaire. The questionnaire will help the researcher attain the objectives; to review the corporate information security challenges arising from the integration of BYOD in the banking sector, to examine the factors of BYOD integration that promotes a sustainable corporate information security, to design and develop the BYOD model and finallyto test and validate the model.

Please, note that all the informationgiven shall be purely used for academic purposes and shall be treated as confidential. Thank you for taking your time to complete the questionnaire and for your cooperation.

Part A: Demographic information

1. Gender of the respondent

   Male [ ] Female [ ]

2. Length of service in the organization

   0-5 years [ ] 6-10 years [ ]

   11-15 years [ ] 16 years and above [ ]

3. Kindly state the category of your age

   Below 25 Years [ ] 35 – 45 Years [ ]

   26 – 35 Years [ ] Above 45 Years [ ]

4. Level of education

   College diploma [ ] Degree [ ] Postgraduate [ ]

PART B: Mobile Device Management

Please indicate the extent to which you agree with the following statements relating to the impact of mobile device management on corporate information security.

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
(a) A mobile device management system is vital in having a sustainable corporate information security					
(b) Enhanced application inventory keeping of all mobile devices is essential					
(c) Computer hardware inventory for BYOD devices enhances information security within the organisation					
(d) Mobile device management tools are essential to ensuring enterprise compliance in relation to users privacy					

PART C: Information Security Policies

Please indicate the extent to which you agree with the following statements relating to the effect of information security policies on sustainable corporate information security.

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
(a) Information security policies are clearly illustrated to all BYOD stakeholders within the organisation					
(b) The institution information security policy documents aid in enhancing sustainable corporate information security					

(c) Having a cyber security framework for the institution supports a sustainable corporate information security					
(d) The information security policies of the institution increase the integrity of the BYOD system					

PART D: Security Culture

Please indicate the extent to which you agree with the following statements relating to the role of security culture on a sustainable corporate information security

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
(a) The existing security culture in the organisation fosters improved corporate information security					
(b) Reported computer security threats are adequately managed by the IT department to ensure sustainable corporate information security					
(c) The financial resources dedicated to corporate information security is sufficient					
(d) The organisations security culture needs to be enhanced going forward under BYOD					

Part E: Employee Education

Please indicate the extent to which you agree with the following statement relating to the effect of Employee Education on a Sustainable corporate information security

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
(a) Employees in the institution have sufficient knowledge regarding sustainable corporate information security					
(b) The level of information security training provided aids in enhancing corporate information security while using BYOD					

(c) The guidelines provided by human resources are congruent with the corporate information security needs under BYOD					
(d) Regular training on computer security while under BYOD is critical for a sustainable corporate information security					

Part F: Sustainable Corporate Information Security

Please indicate the extent to which you agree with the following statement relating to a Sustainable corporate information security

Statement	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
(e) Mobile device management affects sustainable corporate information security of the bank.					
(f) Information security policies on BYOD use affect the sustainable corporate information security of the bank.					
(g) The security culture of the organisation has an impact on the sustainable corporate information security of the bank.					

Thank you for your time and God bless you.