BRING YOUR OWN DEVICE ADOPTION AND INFORMATION SECURITY RISKS AMONG SMALL AND MEDIUM ENTERPRISES IN NAIROBI COUNTY

BY

JANET WALI MWAWALI

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION, FACULTY OF BUSINESS AND MANAGEMENT SCIENCES, UNIVERSITY OF NAIROBI

NOVEMBER 2022

DECLARATION

This research project is my original work and has not been presented for any award in any other university.

Sign Wali. Date 13/12/2022

Janet Wali Mwawali

D61/13450/2018

This research project has been presented for examination with my approval as the University Supervisor

Sign: Lelei Date 11/12/2022

Mr. Joel Kiplangat Lelei

Lecturer

Department of Management Science and Project Planning

Faculty of Business and Management Sciences

ACKNOWLEDGEMENTS

My sincere thanks go out to my supervisor, Mr. Joel Kiplangat Lelei, for his unwavering support, supervision, and guidance as he led me through the research. In addition, I want to express my gratitude to all of the lecturers who served on the research proposal defense panel because their critical analysis and insightful comments aided my presentation. The successful completion of this study would not have been feasible without their thoughtfulness, suggestions, and support.

Lastly, I would like to acknowledge the Dataclave Ltd. fraternity for making my schedule flexible, allowing me to see this project to completion.

Thank you.

DEDICATION

This project is dedicated to my mother, Holiness Mwawali, husband, Michael Okoth, and friend, Jenipher Akinyi for believing in my abilities and cheering me every step of the way. You all were rooting for me even when I was discouraged. Thank you for challenging and supporting my educational pursuits.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ARP	Address Recognition Protocol
BYOD	Bring Your Own Device
CBK	Central Bank of Kenya
CoIT	Consumerization of IT
EIU	Economist Intelligent Unit
ENISA	European Union Agency for Cybersecurity
GOK	Government of Kenya
ICT	Information and Communication Technology
IDT	Innovation Diffusion Theory
IT	Information Technology
MM	Motivational Model
MPCU	Model of PC Utilization
MSMEs	Micro, Small, and Medium-Sized Businesses
SACCO	Savings and Credit Cooperative Organization
SDGs	Sustainable Development Goals
SMEs	Small and Medium-sized Enterprises
TAM	Technology Acceptance Model
TOE	Technology Organization Environment
TPB	Theory of Planned Behavior
TRA	Theory of Reasoned Action
USB	Universal Serial Bus
UTAUT	Unified Theory of Acceptance and Use of Technology
WAP	Wi-Fi Protected Access

ABSTRACT

When it comes to raising capital and keeping up with technology, small and medium-sized businesses (SMEs) face numerous challenges. To address these challenges, they have resorted to allowing employees purchase and use personal devices at the workplace and this is what Bring Your Own Device (BYOD) entails. Although SMEs have been aggressive in BYOD adoption but forget to look at the security part of it. The purpose of the study was to examine the information security risks observed as a result of BYOD adoption among in SMEs in Nairobi County. The study employed a descriptive cross-sectional research approach. 43,539 registered and licensed SMEs in Nairobi County were the subject of the study and 196 of them were sampled. Using a structured a self-administered structured questionnaire, primary data was gathered. The questionnaire was administered to respondents that held positions that gave them intimate knowledge about the information technologies adopted by their respective organizations including owners, directors, IT administrators, program managers, heads of departments, and supervisors. Descriptive and inferential statistics were used to examine the data collected and tables and charts were used to report on the findings. The study revealed that SMEs in Nairobi County have in some way permitted BYOD. It also revealed that there is little if any correlation between the extent of BYOD adoption and application in communication, research, data management and storage, and in networking and information security risks. The study recommended the sensitization of the top top-level management on the phenomenon to appreciate it as a formal concept and fully understand the risks it poses before adoption and the inclusion of training and awareness programs on the same.

CHAPTER 1: INTRODUCTION

1.1 Background to the Study

Technological development has altered the traditional order Information Technology (IT) innovation dissemination from a top-down (organization to workers) to a bottom- up (workers to organization) paradigm (DeHayes, Hoffer, Martin & Perkins, 2014). The falling prices and increased sophistication in consumer devices such as phones and computers have made mobile devices accessible and affordable. Consequently, there has been an increase in computing devices' networking capabilities and versatility thus leading to the Bring Your Own Device (BYOD) phenomenon. BYOD is a trend where employees prefer to purchase and use their appliances such as laptops, phones, and tablets to fulfill their contractual duties (Cisco Systems Inc.,2012), with some organizations even purchasing these devices for their employees and allowing them to use them for both organizational and personal use.

The Kenya Cyber Security Report (2018) analysis reveals that companies in Kenya today have implemented BYOD programs encouraging their employees to use personal IT gadgets at the workplace. 65 percent of the participants acknowledged that their organizations allowed the use of BYODs. The figure represents a 24 percent increase from the figure reported by the Kenya Cyber Security Report (2017). These statistics support that Kenya is at the cutting edge of technological advancements and hence the title of Africa's 'Silicon Savannah.' According to Kenya's Digital Economy Blueprint, to enhance the country’s e-readiness, the Government of Kenya (GOK) has made significant investments in information and Communication Technology (ICT) and has acknowledged the sector as a critical contributor to the country's GDP. Digitization has been expedited by the coronavirus outbreak, creating new prospects for telecom operators as well as hardware and software dealers ("Kenya - Information, Communications, and Technology (ICT)," 2021). Fast and dependable connectivity, according to the Economist Intelligent Unit (EIU), remain essential for organizations, consumers, and policymakers as they work to address the pandemic.

Scholars have argued that BYOD in the corporate environment makes sense from a business and IT perspective. Mbalanya (2013) highlights that BYOD increases employee productivity and collaboration, reduces IT capital expenditure and ongoing support costs, and allows an organization to keep up with technology. However, prematurely allowing BYOD into a business introduces risks that may compromise the organization's assets security (Oliver, 2012). Evans (2020) asserts that BYOD could threaten IT and information security and put a company's systems at risk, if not properly regulated. Security risks begin when confidential corporate data is stored on an employee device that the organization has little or no control over. Security risks associated with BYOD include network vulnerabilities, data leakage, malware, targeted attacks, and loss or theft of devices (Garba, Armarego, Murray & Kenworthy, 2015). Therefore, adopting BYOD calls for IT enterprise managers to navigate and mitigate the challenges and risks. IT security scholars have recommended several security measures to minimize BYOD risks. The proposed measures include the management of these devices through policies, security awareness training programs, and the implementation of a mobile device management system. According to the Kenya Cyber Security Report (2018), 56 percent of the participants in the survey acknowledged that their organizations have a best practice policy for BYOD. The figure represents a 3 percent decrease from the figure reported by the Kenya Cyber Security Report (2017).

Minimal investigations have looked at the BYOD phenomena and its security challenges from perspective of Small and Medium-sized Enterprises (SMEs). The latest National Economic Survey

Report from the Central Bank of Kenya (CBK) states that SMEs make up 98 percent of all businesses in Kenya. Micro, small, and medium-sized businesses (MSMEs), the bulk of which belong to the informal sector, generate about 40 percent of the GDP. Despite the immense economic contribution, Kenya's SMEs face numerous challenges. SMEs are more likely to adopt BYOD based on the challenges they face in the market space. The Deloitte Kenya Economic Outlook Report (2016) states that challenges faced by SMEs include inadequate capital, limited market access, rapid changes in technology, inadequate knowledge and skills, and poor infrastructure. Therefore, SMEs adopt BYOD to save on costs, keep up with technology, foster learning, and skills development, and enhance reach. This research will analyze the BYOD environment of SMEs based in Nairobi County.

1.1.1 Bring Your Own Device

Whilst the idea of BYOD first appeared in 2003, it was appreciated as a concept in 2011 (Leavitt, 2013). Workers now frequently utilize their gadgets to conduct their respective job obligations (Harris, Ives & Junglas, 2012). According to Deloitte (2013), BYOD is the use of personal devices to access a business network by employees. It is the process that outlines how users render their personal devices for business use (Doargajudhur & Dell, 2018). Lee et al., 2016 define it as a concept where individually owned mobile appliances are utilized for enterprise and personal reasons. This study adopted the BYOD definition as a practice whereby the employer permits the employees to use personal devices to access the organization’s network and fulfill their contractual obligations.

Approximately 85 percent of businesses globally have implemented at least one business process to accommodate BYOD (Mordor Intelligence, 2020). Employees are finding it more convenient to have a single device rather than one for work-related tasks and another for personal use. They believe that in doing so, they will be more productive, collaborative, and flexible with access to communication platforms such as email, among other business applications, outside working hours (Garba et al., 2015). Then again, the organizations believe that BYOD supports the cost-cutting and competitive advantage objectives (Garba et al., 2015). These form the factors that encourage BYOD adoption. It is no more a matter of adopting a BYOD strategy but how it can be done more effectively to gain all the benefits that come with it (French, Guo & Shim, 2014). While the benefits are apparent it is essential to examine the extent of BYOD adoption and the factors that encourage BYOD adoption.

Mbalanya (2013) examined the extent of BYOD adoption by analyzing how employees are permitted to perform operations using their mobile devices. These operations include access to corporate files and documents, video conferencing, taking work calls, email correspondence etc. Arwa (2014) defined BYOD adoption in the banking sector by looking at how employees used their personal devices to send or receive work emails, call bank customers, organize calendar activities, and scan client documents. Kutoto (2020) added on to what Mbalanya (2013) and Arwa (2014) by including the use of employees' devices in executing the organization's social media campaigns, accessing the organization's intranet and extranet, and storing company data.

1.1.2 Information Security Risks

Information is a critical asset to an organization that warrants protection. Business entities owe it to their stakeholders and shareholders to protect corporate information. Everything that threatens the confidentiality, integrity, and availability of corporate confidential information is an information security risk (Nieles et al.,2017). Threats, vulnerabilities, and impact are the three key ideas that shape information security risks. Threats take advantage of vulnerabilities and would cause losses if they occurred. A vulnerability is a flaw that a threat could exploit in an information system, system security protocols, controls in place, or implementations, as per Gantz and Philpott (2013). The resulting loss or potential loss brought on by a threat exploiting a vulnerability is the impact (Talabis & Martin, 2013).

Previously, studies on information security risks were from a technical viewpoint. Researchers' focus has however, shifted to investigating the management's role in information security as a result of growing security requirements (Soomro et al., 2015). Security risks include malware, phishing, targeted attacks, data exchange interception, loss/theft of gadgets, insider actions, and user policy violations. With companies still facing these risks, the statistics indicate that organizations have to enhance their controls to minimize these risks better. Management plays a key role in creating an effective information security culture that could significantly decrease data breaches in businesses (Da Veiga et al., 2020). Insiders are the predominant weakness in properly securing information assets (Crossler et al., 2013). Therefore, to improve compliance with information security policies, information security training and awareness initiatives must be implemented (Ayyagari & Figueroa, 2017).

Information security is a well-discussed topic in different contexts. Mbalanya (2013) measured information security risks by examining the extent to which threats have been experienced. Wangutusi (2015) operationalized information security risks by analyzing the degree of concern associated with threats and vulnerabilities. Soomro et al., 2015 reviewed the need for an integrated approach to information security. In this case, the researchers measured information security risk by examining the availability of information security policies in organizations, strategic alignment of information security and the overall organization strategies, the extent to which the underlying security issues are understood, and the availability of training programs on the same. Cilliers (2019) investigated information security from the context of wearables in healthcare. The researcher measured information security risks by gauging the need for wearable device users to protect information assets, and the knowledge and comprehension of the information security issues and security policies in place.

1.1.3 BYOD Adoption and Information Security Risks

The association between BYOD adoption and information security risks can be confirmed empirically in various contexts. In the context of SMEs in Tanzania, Kabanda and Brown (2014) found a positive association between the two factors. The researchers realized the effect of the BYOD phenomenon on information security when corporate data is distributed to devices not controlled by the organization's ICT department. Boateng & Boaten (2016) explored the risks, threats, and vulnerabilities associated with adopting BYOD. Findings indicate that the respondent's opinion of BYOD use presented cybersecurity challenges to information assets.

Ounza, Liyala, and Ogara (2018) considered the security challenges posed by BYOD at Kenyan universities. The researchers cited lack of awareness, difficulty managing different devices and platforms, and loss of device control as information security risks posed by BYOD adoption. The deduction from previous studies confirms that BYOD adoption has significant benefits; in contrast, it involves diverse information security and privacy concerns. Baillete and Barlette (2018) uncovered a neutral relationship between BYOD adoption and information security threats as they hold that BYOD opportunities and benefits outweigh the information security threats.

1.1.4 Small and Medium Enterprises (SMEs) in Kenya

A wide scope of businesses in Kenya is SMEs. They are a key driver toward achieving Sustainable Development Goals (SDGs) in Kenya (Mutegi, 2015). There is lack of a definite meaning of SMEs in Kenya, seeing that there is no standalone law on SMEs (Mputhia, 2020). Most scholars define them based on the number of employees, while others take the profit margins point of view. Table

1.1 below shows the distinction between micro, small and medium enterprises as per the Kenya Micro and Small Enterprise Act, 2012. Furthermore, the Public Finance Management Bill (2019) defines a medium enterprise as a firm that has 51–250 employees and an annual revenue of up to Kshs. 100 million (Mputhia, 2020).

Table 1.1: Definition of Micro, Small and Medium Enterprises in Kenya.

Type of Enterprise	Number of employees	Annual Turnover (Kshs.)
Micro	<10	<500,000
Small	10<x<50	500,000<x<5,000,000
Medium	50<x<250	5,000,000<x<100,000,000

SMEs play a paramount role in reducing the unemployment levels among the Kenyan youth and influence income generation. Their potential needs to be tapped to boost our economy's status. Challenges encountered by SMEs include limited resources, inadequate knowledge of management, and the integration of information technology in the business's daily operations (Deloitte Kenya, 2016). BYOD can come in and alleviate these challenges and even accrue more benefits for the businesses. The reason behind this is the fact that the concept will help businesses significantly reduce their operational and setup costs while giving them access to up-to-date technology.

The research specifically emphasizes the SMEs particularly those in Nairobi, the capital city of Kenya because they make a significant contribution to the country's economy and are advantageous to adopt recent technology because of their structure.

1.2 Statement of the Problem

In the current era, it is evident that BYOD programs are transforming the workplace by extending the notion that employees worldwide would prefer to work from anywhere and anytime without restrictions as far as connectivity is concerned. Forrester's research, 2012 indicates that 50 per cent of knowledge workers utilize their personal devices for work. Therefore, it is critical to highlight that the BYOD trend presents a significant opportunity to transform business models, enable agility and flexibility, and encourage innovation in customer interactions. While employees enjoy the freedom and convenience of BYOD, the phenomenon has raised significant information security risks that must be addressed (Obote, 2019). These risks include malware, phishing, targeted attacks, and vulnerabilities, loss or theft of devices, insider threats, and user policy violations. Kamau (2013) states that the most significant limitation of BYOD adoption is the information security risk it poses. However, he holds that the information security risks are inherent but can be reduced or mitigated. Shondo (2019) agrees with Kamau (2013) and Obote (2019) and posits that without safeguards to protect data, information security risks become inevitable. Kutoto (2020) concluded that the lack of sound policies to direct personal devices use for work exposes organizations to information security risks they may not have anticipated. Therefore, more effort must be put in place to manage BYOD adoption, hence why BYOD adoption and the information security risks it poses should be studied together.

SMEs have been aggressive in BYOD adoption but forget to look at the security part of it. Amrin (2014) concluded that SMEs lack sufficient attention to IT security, with the related obligation often unassigned or allotted to someone without suitable qualifications. For instance, according to information from the CBK, targeted attacks on SACCOs' lax controls and unreliable systems resulted in losses of $947,528 over the course of 17 months ending in March 2021 (Namunwa, 2021). 43 percent of total cyber-attacks target SMEs thus making them 6 times more vulnerable to information security risks than bigger corporations (Symantec, 2016). SMEs adopt BYOD for the perceived benefits such as cost savings on IT infrastructure and support, access to up-to-date technology, increased employee productivity and efficiency, and a competitive edge. While BYOD adoption can provide such advantages, the surge in information security concerns must be accompanied by laws and policies that offer broad legal defenses against threat actors. Therefore, while putting information security risks in BYOD adoption abreast, SMEs will be in a better position to minimize the prevailing risks, thus avoiding any losses.

Studies by Ounza et al. (2016) and Oonge, Muhambe, and Ratemo (2021) have shown that organizations in Kenya have adopted BYOD without management authorization or without considering security risks. John Kutoto (2020) notes that only 16 percent of NGOs in Kisumu county have formalized the BYOD process by having the policy to guide implementation, thus rendering the usage and related security concerns vague. Whereas previous studies focused on learning institutions and NGOs, this study focused on SMEs within Nairobi County. No local study specific to the SME sector has been done. This research closed the gap by responding to the following query: What are the information security concerns connected to SMEs in Nairobi County adopting BYOD?

1.3 Research Objectives

The study's primary goal was to examine the relationship between BYOD adoption and information security risks among SMEs in Nairobi County. The precise objectives are to:

1. To establish the extent of BYOD application.
2. To establish the motivating factors for BYOD adoption.
3. To determine the relationship between BYOD adoption and information security risks.

1.4 Value of the Study

This investigation's value is contributing to scholarly works on adopting consumer technologies at the workplace. It will provide statistical evidence to explain the trend, including the motivation, benefits, risks, and challenges. First, SMEs management can make strategic decisions on BYOD adoption while being aware of the information security risks its poses. The research results will enable them to craft policies that will maximize the benefits of BYOD. Second, consumer technology device manufacturers and software developers will find this research valuable as it will give insight into the employees' preferences and thus produce superior products that the employees need. As creatives, the research will inspire these developers and manufacturers to produce more innovative ideas to help organizations quickly adopt the trends in the IT world and change business processes.

Additionally, this research will be invaluable to scholars who shall use it to weigh in on the results and discover areas for further research in other industries. Policymakers in the Information Communication Technology Ministry will consider the study's findings in the decision-making process regarding adopting BYOD and its policies.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter delivered the evolution of BYOD and theoretical framework surrounding its adoption among different SMEs in Nairobi. Moreover, this section explored previous studies to establish the extent of BYOD adoption, motivating factors, and information security risks of adopting BYOD.

2.2 Theoretical Review

2.2.1 Technology Organization Environment (TOE) Framework

The TOE model, created by Tornatzky and Fleischer in 1990, suggests that an enterprise's context affects how technological advances are adopted and implemented. This organizational level theory holds that a firm's setting consists of three factors that affect adoption choices namely technology, organizational, and ecological factors (Tornatzky, Fleischer & Chakrabarti, 1990). The framework proposes that BYOD adoption is influenced by elements from these three constructs. In the technological context, an organization would decide whether or not to adopt BYOD based on the technologies that are pertinent to the firm- both in use and those available in the market but not necessarily in use (Baker, 2011). The firm's features and resources, such as the networks that connect employees' internal communication processes, its size, and the underutilized resources, form the organizational context (Baker, 2011). Finally, the environmental context is where an organization conducts its activity. It encompasses the industry's structure, the regulatory landscape, and the existence or absence of technology service suppliers (Venkatesh & Zhang, 2010).

Given the reality of the contexts proposed by the TOE framework, there has not been much criticism raised. Thus, the TOE framework has barely changed since its establishment. There have been no additional constructs created over the years. The lack of development results from the framework being considered a generic theory which complements existing theories on how innovations are adopted, as opposed to providing a competing theory (Baker, 2011). This framework is relevant to the BYOD adoption case as it points out the factors that need to be considered before BYOD adoption. The deduced drivers for BYOD adoption include access to technology relevant to the firm, cost reduction techniques, the need to enhance employee productivity, efficiency, and collaboration, and gain a competitive edge in the industry.

2.2.2 Technology Acceptance Model (TAM)

The TAM concept provides an explanation of how innovations are adopted by users. According to the model, a person's desire to utilize certain technology depends on how beneficial and simple it is to use (Davis, Bagozzi & Warshaw, 1989). These two aspects are highly influenced by political, social, and cultural factors. Despite the frequent use of the theory, it has been widely criticized by other scholars that claim that there is more to it than the relative advantage and simplicity of usage (Venkatesh & Davis, 2000). Hence, many researchers have, over time, modified TAM to include other relevant variables. For instance, in 1998, Agarwal and Prasad added compatibility to the model. Chau and Hu (2002) combined TAM with peer influence. Franco and Roldan (2005) found that a group of users magnified usefulness and behavioral intention with a similar goal. From these citations, it is evident that TAM has been assessed, verified, modified, and replicated empirically with criticism on its debatable heuristic usefulness, limited explaining and predictive capacity, frivolity, and lack of practical value.

In summary, the TAM theory highlights the considerations that predict the adoption and acceptance of BYOD, including its relative benefits and simplicity of usage.

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

The UTAUT model explains users' initial intentions to use new technologies and their successive usage patterns. It combines other user acceptance models to give a better understanding of the likelihood of users accepting technology (Venkatesh, Morris, Davis & Davis, 2003). These models include among others, the Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), Motivational Model (MM), Theory of Planned Behavior (TPB), Model of PC Utilization (MPCU), and Innovation Diffusion Theory (IDT) (Venkatesh et al., 2003). As direct predictors of BYOD adoption, the theory highlights four main constructs: performance expectancy, effort expectancy, social influence and facilitating conditions. Furthermore, the theory contends that age, gender, experience, and volunteers of usage indirectly influence these constructs.

Although the theory presents a comprehensive front due to the inclusion of other models to develop the constructs, it has also been subject to criticism from other scholars. For example, Van Raaji and Schepers (2008) critiqued the model by pointing out that since it achieves a high coefficient of determination (R2) when moderating important relationships with up to 4 variables, it is considerably less frugal than compared to TAM. The scholars also noted that it was difficult to categorize and label the psychometric construct because a number of diverse variables were merged to form and describe one construct. However, despite acknowledging that the UTAUT model is comprehensive, Bagozzi (2007) provides a model with 41 and 8 independent variables for predicting intentions and behavior, respectively. The mismatch in these variables brings a state of chaos. Despite the criticism, the model is relevant to the study as the proposed constructs are determinants of BYOD adoption and acceptance.

2.2.4 Diffusion of Innovations Theory

This model originated from Rogers and dates back to 1962. It describes how an idea picks and spreads among a particular demographic or social system over time. The diffusion results in the adoption of the new idea as a social norm. The author posits that users' ability to adopt technology will depend on their knowledge in conjunction with other contextual factors (Rogers, 2003). The diffusion of innovations theory is applicable in assessing both individual and organization levels of adoption behavior (Lai & Guynes, 1997).

The innovators, early adopters, early majority, late majority, and laggards categories were established by Rogers. Moreover, according to Rogers (2003), there are four stages in which an innovation is adopted: knowledge about the necessity for the innovation, choice to accept or reject the innovation, debut usage of new technology to try it, and continuous usage of the technology. The acceptance of an innovation is primarily influenced by five considerations: relative advantage, compatibility, intricacy, trialability, and observability.

Critiques of the theory highlight that it fails to recognize other environmental factors that might affect the adoption by only concentrating on individual characteristics (Lee and Cheung, 2004). Others suggest that the theory should be coupled with other theories to strengthen its position for a holistic view of technology innovation adoption. According to Lyytinen and Damsgaard (2001), some theoretical notions that assist in explaining how intricate networked technologies diffuse are not addressed by the theory. These scholars recommend a reconsideration of several basic premises of this theory. Nevertheless, the diffusion of innovations theory predicts that some organizations and individuals in the social system are more likely to embrace BYOD than others based on the factors present in their environment.

2.3 Adoption of BYOD

2.3.1 Extent of BYOD Adoption

In recent years, the development of collaborative and interactive applications has led to the concept of consumerization of IT (CoIT)- a trend that is both intriguing and challenging for IT organizations when employees invest resources to gain products that they can leverage in getting their job done (Unisys, 2010). Historically, organizations had complete control and ownership of the technologies used at the workplace, such as mainframes, computers, telephones, workstations, and time-sharing management systems. Currently more workers prefer to utilize their mobile devices for work thus wiping out this trend (DeHayes, Hoffer, Martin & Perkins, 2014). They perceive that the applications, devices, and services they use at home to complete their contractual tasks are easier and more convenient to use than the IT framework provided at work. Business entities offer BYOD programs to keep up with the trends. These programs let staff members conduct business operations and processes using personal gadgets such as cellphones, tablets, computers, hard drives, and USB sticks (Sadiku, Nelatury & Musa, 2017).

Potential effects of cellphones at the workplace are a contentious topic. The term ‘smartphone’ was established years ago, but once Apple introduced the smartphones to the general public in 2007, it was a game changer. The first digital phones operated as enterprise devices for making and receiving voice calls. However, over time, people realized they could potentially help in the business world. Pitichat (2013) posits that by allowing employees to use smartphones for work, leaders will benefit as their employees will develop their satisfaction and engagement at work. Furthermore, Li and Lin (2019) found that employee’s perceptions of their job performance and workplace social capital appear to improve as a result of workplace smartphones dependency.

The BYOD concept revolves around mobile devices purchased by users and used for official work. Ophoff and Miller (2019) emphasize the need to understand where BYOD fits in an organization before implementation. According to IBM, the phenomenon must be implemented with varying access and data storage levels. Additionally, there needs to be policies and guidelines in place to avoid misuse of these devices.

BYOD has been applied in completing various tasks at the workplace. By examining whether employees utilize their mobile devices for work and the precise tasks they perform using those devices, it is possible to determine the level of BYOD adoption (Mbalanya, 2013). This study will establish the extent of BYOD adoption by observing whether employees use personal mobile devices at the workplace and which duties they can apply these devices at the workplace. Previous studies by Mbalanya (2013), Arwa (2014), and Kutoto (2020) provide a list of duties in which employees can use their mobile personal devices at the workplace, such as in e-mail correspondence, accessing the corporate network, and social media marketing. For this research undertaking, we shall consider four broad categories where BYOD can be applied in the workplace. These categories include communication, research, data management and storage, and networking.

2.3.2 Motivating Factors for BYOD Adoption

The dynamic nature of the business environment, including product and service offerings, calls for employees to be flexible, efficient, and more productive. At the same time, innovations meant for the consumer markets have increasingly made their way into the market space (Doargajudhur & Dell, 2018). New technology is emerging to consumers first, meaning that employees already have experience with these new technology innovations. Since workers are already accustomed to the gadgets, BYOD allows them to be productive right away, thus increasing their morale and engagement (Weiß & Leimeister, 2012). As a result, the amount of time they need to train is cut down which boosts their efficiency and productivity. According to Kamau (2013), BYOD adoption is a crucial element that seeks to enhance employees' and organizations (by extension) productivity. Managers and supervisors have reported rising productivity, efficiency, and a willingness to work on projects after work hours. Accessing the company network using personal devices allows employees to work at any time, thus alleviating the limitations posed by a 9:00 AM to 05:00 PM workday.

Furthermore, the Covid-19 pandemic made organizations rethink their office spaces. 16 percent of companies globally were recorded to be fully remote, meaning that the number of employees working remotely is continuously growing (Owl Labs, 2021). Implementing fully remote or hybrid arrangements creates the need for employee collaboration to improve how teams work together to solve problems. BYOD presents a viable solution because by utilizing their gadgets while working together on assignments, employees find themselves using their devices more effectively (Pemarathna, 2020). A strong collaborative culture within the organization encourages problem-solving, fosters peer learning, and increases the organization's potential for change.

Organizations strive to increase revenues and lower business costs. Lowering business costs can prove to be an essential factor in expanding their margins. Technology is an investment that can optimize processes and improve performance (Siddiqui, 2014). However, IT investment levels vary from sector to sector in the same industry. BYOD allows organizations to lower IT investment costs (Siddiqui, 2014). Employers formerly had to cover the hardware, software, and other contract costs in order to use mobile devices. Effective BYOD policies enable organizations to significantly cut costs associated with supplying devices to all employees, training them on how to use them, hiring IT support teams, and the cost incurred in the maintenance and upkeep of the devices and appliances (Pemarathna, 2020).

Moreover, organizations struggle to get the latest devices with updated features due to the increase in innovations in technology and limited resources. Employees with experience with ICT innovations used for personal tasks wish to have a similar user experience in corporate environments because they believe their infrastructure will fulfill their expectations (Doargajudhur & Dell, 2018). Therefore, a sound BYOD policy will allow organizations to utilize newer devices and their cutting-edge features. Employees will be accountable for staying current with technology if they are allowed to bring and use their devices to work (Weiß & Leimeister, 2012). Therefore, workers are not required to wait for respective employers to upgrade all their devices. Employees are more likely to be vigilant about keeping their devices up-to-date and installing the latest updates. Using the latest technology without more costs, benefits businesses of all types and sizes (Siddiqui, 2014).

Finally, the need to have a competitive edge is a key motivator for BYOD adoption. According to Miller- Merrel (2012), organizations which neglect latest technological advancements miss on significant competitive advantages. BYOD adoption gives the organization a competitive edge by ensuring that it incorporates the latest technology tools and platforms to make all the business functions efficient (Miller-Merrell, 2012). Additionally, adopting BYOD enables organizations to attract the best pool of employees from the market because of the flexibility in working hours and the devices and appliances used. Flexibility is an attractive feature to prospective employees in the job market. Most people prefer to have flexibility in executing their contractual duties. Additionally, as mentioned earlier, it enables organizations to save on costs, thus setting them apart from their competitors (Siddiqui, 2014). Therefore, organizations that have implemented BYOD have the upper hand as compared to other market players in the market space.

2.3.3 Information Security Risks

Organizations are embracing the BYOD trend to attain benefits such as cutting IT expenditure, enhancing employee productivity, collaboration etc. However, studies depict that these benefits come at a cost by exposing an organization to new risks (Akin-Adetoro & Kabanda, 2021). A practical BYOD framework should ensure that the objectives of the three information security pillars are met. Failure to that, BYOD presents risks that must be addressed to ensure security in the business environment. Information security risks intrinsic to the BYOD framework include data leakage, malware, social engineering, phishing attacks, targeted attacks and vulnerabilities, unauthorized access and manipulation of interception and spoofing of communication, devices loss or theft, malicious insiders, and policy violations by users (Lyndon, 2014).

2.3.4.1 Data Leakage

Organizations deal with confidential data about their clients, vendors, strategies, and so on. Data leakage refers to unauthorized data transmission from an organization to an external party (Ogie, 2016). There are a number of ways that data leakage can happen when a company adopts a BYOD framework, and the impact can range from low to high. First, mobile devices could get lost or stolen, and the stored data can be accessed if not encrypted (Ogie, 2016). Second, malware like Trojan Horse viruses, which threaten data security, may already be present on the machines (Ogie, 2016). Once this data leaks, it causes significant damage to the organization’s reputation, compromises its competitive edge, and imposes substantial financial losses due to the additional organizational costs to cover a data breach depending on the extent of the breach.

2.3.4.2 Malware

BYOD adoption has accelerated the growth of malware. It is an intrusive software designed by cyber criminals with the intention of spying on users, stealing their data, and damaging the system or device (Watchguard, 2013). Examples of common malware include viruses, worms, spyware, ransomware, and adware. According to Alcatel-Lucent (2013) analysis, the rising popularity of BYOD accounts for 11.6 million gadgets being infested with spyware at any given moment.

2.3.4.3 Social Engineering and Phishing Attacks

Phishing is a social engineering attack in which perpetrators use emails or websites to get personal information while assuming the identity of reliable businesses or people. Attackers utilize human interaction to gather or compromise information about a company or its computer systems in a social engineering attack. Social engineering attacks primarily deploy non-technical methods to access buildings, systems, and information (Carranza, Carranza & Zaidi, 2019). Passwords may be unsafe, the user may download apps from unknown sources, and a friend or a family member may borrow the device. All these pose security risks when the same device is used professionally and privately, as in BYOD environments. Additionally, employees in organizations that have adopted BYOD hardly subject their devices to rigorous security standards that apply in the business environments (Carranza, Carranza & Zaidi, 2019).

2.3.4.4 Targeted Attacks and Vulnerabilities

Targeted attacks occur when perpetrators infiltrate an organization's network environment to gain access to confidential information with the intention to destroy, modify or extract it for illegal use (Bello, Armarego & Murray, 2015). In 2021, eight (8) Kenyans launched a targeted attack against Equity Bank. They infiltrated the bank's network and hacked into the accounts. The hackers then funneled cash to Rwandans, who were then to withdraw the funds through Eazzy banking and ATMs (Business Daily, 2021).

Along with targeted attacks, employees in BYOD environments frequently put the security of their particular firms at risk by failing to update their devices. These devices may have vulnerabilities in their unpatched or out-of-date software that could be exploited by malicious individuals.

2.3.4.5 Data Communication Interception

Continuous interception of wireless data streams has become a significant security challenge to BYOD environments. Data communication interception is defined by Evripidis (2008) as the prevention of data flow, to and from the device and the remote alteration of messages. It poses a risk to wireless networks that BYOD devices rely on (Bello et al., 2015). Interception of data communication is a breach of confidentiality since it gives unauthorized users access to data, applications, or environments (Evripidis, 2008). Among the many ways this risk manifests itself are unauthorized viewing and copying of files, listening in on phone calls, and reading emails. Consider the “Hole 196” vulnerability in the Wi-Fi Protected Access (WAP) 2 security protocol. It allows the users to access other resources through WPA 2 and a wireless network and allows for Address Recognition Protocol (ARP) spoofing (Kohlios & Hayajneh, 2018). Organizations connected via “Hot 196” create an opportunity for attackers to take advantage of this vulnerability to retrieve other users’ personal information as well as to launch malicious threats into the wireless network.

2.3.4.6 Loss/Theft of Devices

BYOD allows employees to store, access, and process confidential organization information using personal mobile devices. In most cases, employees use these devices to access their organization’s network automatically, therefore, if these devices end up in the wrong hands, they may be used for fraud or other illegal activities. Criminals may steal these devices for their value. However, some criminals steal the devices to access personal data, which is more invaluable (Garba et al., 2015). A newspaper article reports the recovery of three hundred stolen phones, one laptop, and thumb drives during a sting operation (Kimatu, 2021). The article depicts how mobile devices could easily get lost or stolen.

2.3.4.7 Insider Threats

A situation whereby an insider intentionally or accidentally compromises the security of an organization’s operations or assets is known as an insider threat. More often than not, the motivation behind insider threats includes disgruntlement, revenge, and financial gain. As per the Kenya Cyber Security Report, 2015, employees and other insiders were cited to be responsible for more that 80 percent of system- related fraud and theft (Serianu Ltd., 2015). Insider threats, according to over three-fifths of IT experts, are harder to detect than third party malicious attacks (Serianu Ltd., 2015). Since mobile device users can access organizational systems and resources from any location, BYOD makes insider threats easier to execute. As a result, malicious employees run the risk of executing virus attacks, phishing scams, eavesdropping, and even organize for the theft of mobile devices.

2.3.4.8 User Policy Violations

BYOD renders it more challenging for enterprises to impose rules and regulations on workers and reduces the institution's control over the technologies used by workers to conduct business. Mobile devices can be exposed to vulnerabilities if they are used to access and download web content that might include malware from ‘untrusted certificate’ websites or if antivirus and firewall software are disabled. An example is the Citi Bank 2011 breach which occurred as a result of a technical flaw in Citi Cards’ Account Online Web- based System and exposed more than 360,000 credit cards issued by the bank. The bank reported that the breach occurred as a result of one of the employees utilizing a peer-to-peer (P2P) file-sharing program from a BYOD laptop device on their network, and that they had been aware of the vulnerability since 2008 (Kitten, 2013).

2.4 Empirical Review

Empirical studies on the BYOD phenomenon show that BYOD adoption is growing among employees and organizations. Against this background, most studies indicate that BYOD adoption is employee-driven and point out that information security concerns were the main barrier. BYOD has become a key factor in business plans and a popular research topic because studies reveal that more people will keep using personal devices for work related activities.

To understand how the context that SMEs operate in shapes and is shaped by BYOD practices, Kabanda and Brown (2014) looked into BYOD practices used by Tanzanian SMEs. The investigation identified three main themes associated with BYOD practices among Tanzanian SMEs. First, BYOD allowed employees to perform work-related tasks on personal devices, whether or not the company's network was being accessed. Second, BYOD offers the firm economic savings by shifting the burden of maintenance to the end user. Lastly, policies are necessary for successful BYOD adoption since employees' desire to use their devices in accordance with the rules established for them can be used to measure the effectiveness of a BYOD program.

The researchers connect the BYOD phenomenon to information security concerns like data theft, lost/stolen devices, and compliance issues because corporate data is transferred to devices not controlled by organizations' ICT departments. The researchers recommend using policies to safeguard security and govern liability to mitigate identified risks.

Francis E. Boaten (2016) shows that IT functionaries and security professionals who manage various enterprise networks perceived that BYOD adoption poses cybersecurity challenges to corporate information assets. The study found that employees use their devices on business networks without the management being aware. Furthermore, most firms lack explicit BYOD policies which poses a security risk to company information. The scholar found out that data leaking was a serious concern which was in line with the findings of an investigation of smartphone security risks by the European Union Agency for Cybersecurity (ENISA) in 2010.

For management, BYOD has created a twofold security dilemma, according to Baillete and Barlette (2018). The researchers hold that the benefits of BYOD include reduced costs, improved organizational benefits from embedded innovations, and more employee autonomy and motivation. The threats identified in the study include the increased complexity of network protection, lost/stolen devices, targeted attacks, malware, and difficulty in monitoring use and adherence with organization rules and guidelines. According to the study, organizational managers mistakenly believe that their company is protected or that the benefits of BYOD exceed the risks, which leads them to ignore BYOD information security vulnerabilities. Therefore, they primarily focus on the above-mentioned opportunities without putting the necessary precautions in place to deal with the threats and vulnerabilities.

Akin-Adetoro and Kabanda (2021) conducted qualitative research to establish contextual factors influencing BYOD adoption in SMEs in South Africa. The researchers used semi-structured interviews as the data collection tool. The research concluded that organizational or environmental factors are the contextual elements driving BYOD adoption among SMEs. Therefore, for an SME to adopt BYOD, organizational and environmental readiness are prerequisites. These elements were also explored in terms of opportunities and challenges. Business and human resources, employee pressure, and sociocultural factors are potential opportunities for BYOD adoption whereas the challenges include a lack of institutional control, lack of technological readiness, poor management, lack of support from the industry and government, and lack of knowledge of the BYOD phenomenon.

Ounza et al. (2018) posit that majority of businesses that use BYOD are subject to widespread IT security risks. Their study focused primarily on the security issues that Kenyan higher learning institutions are facing as a result of BYOD implementation. IT security challenges uncovered during the study included a lack of user awareness, given that users present a vulnerability even in the most complex systems. In addition, the universities used in the study indicated that they found it difficult to maintain inventory of the personal devices used because they the users frequently brought more than one device with them when they utilized the network. Lastly, the study drew attention to the fact that Kenyan universities lack visibility and control over the devices connected to their networks, thus creating loopholes for information security risks. Based on the unique set of challenges identified, these researchers recommended frequent risk audits and the placement of adequate security measures to counter the challenges.

Moreover, Oonge et al. (2021) surveyed three (3) Kenyan public universities to examine the risks and challenges that higher education institutions experience while adopting BYOD. The study's three hundred and eighty-nine (389) participants echoed that the biggest threat to information security comes from insiders. Other security challenges identified include loss of device control and difficulty implementing all the security tools for all the unique personal devices used to access a network. The researchers recommended that the institutions improve their network infrastructure with top management support by putting in place adequate security measures that are easy for users to understand, developing programs to educate users about all the vulnerabilities that exist and how to prevent them from happening, and conducting regular system audits.

John Kutoto (2020) focused on BYOD adoption among NGOs in Kisumu County. He discovered that the NGOs allow the use of personal devices for work, and a few have an ICT department supporting these devices. However, only 16 percent of the NGOs had formalized the process with a policy to guide adoption and implementation, thus rendering the usage and related security concerns vague. The findings collaborate with Kamau's (2013) findings, where he examined the phenomenon in an exploratory study. He advocated for a comprehensive strategy that centers the creation of personal device usage rules and guidelines arounds the needs of the workforce.

2.5 Conceptual Framework

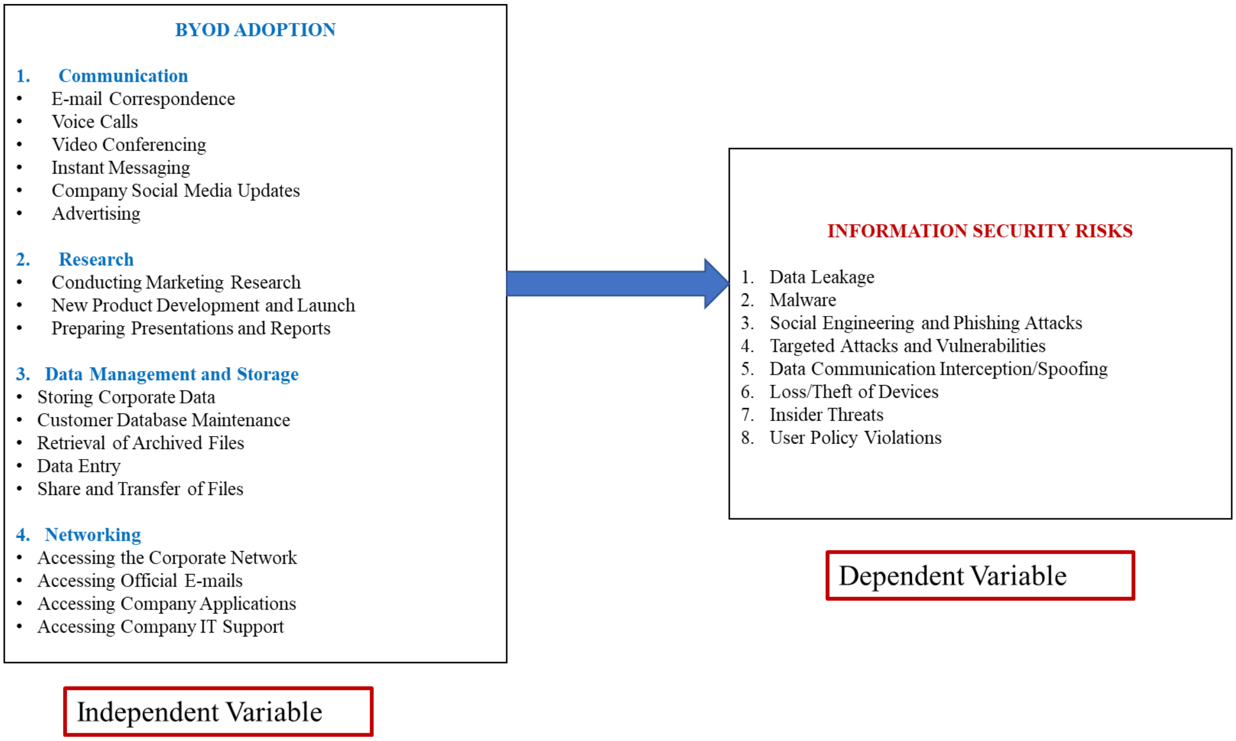
BYOD ADOPTION
1. Communication
• E-mail Correspondence
• Voice Calls
• Video Conferencing
• Instant Messaging
• Company Social Media Updates
• Advertising
2. Research
• Conducting Marketing Research
• New Product Development and Launch
• Preparing Presentations and Reports
3. Data Management and Storage
• Storing Corporate Data
• Customer Database Maintenance
• Retrieval of Archived Files
• Data Entry
• Share and Transfer of Files
4. Networking
• Accessing the Corporate Network
• Accessing Official E-mails
• Accessing Company Applications
• Accessing Company IT Support
Independent Variable
INFORMATION SECURITY RISKS
1. Data Leakage
2. Malware
3. Social Engineering and Phishing Attacks
4. Targeted Attacks and Vulnerabilities
5. Data Communication Interception/Spoofing
6. Loss/Theft of Devices
7. Insider Threats
8. User Policy Violations
Dependent Variable

Figure 1:Conceptual framework for the study

2.6 Summary of Literature Review

This chapter examined the extent of BYOD adoption and the motivating factors that support its implementation in organizations. It covers research studies on the subject, many of which have not yet been conducted in the SME context. The elements discussed were backed up by theories and frameworks used to explain innovation adoption and user acceptance of these innovations. The chapter also looked at the information security risks posed by adopting BYOD in the workplace.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

The term “research methodology” refers to a methodological approach to solving a problem in research. Therefore, this chapter includes the descriptions of the study’s population, sampling, data collection and analysis procedures.

3.2 Research Design

The overall strategy for data collection, measurement, and analysis is known as research design (Kombo& Tromp, 2006). This study utilized a descriptive cross-sectional research design. In this approach, a phenomenon is studied at a particular point in time for a specific population.

3.3 Population

The entire set of elements that researchers are interested in studying to get to a conclusion is referred to as the target population. SMEs in Nairobi County that are registered and licensed made up the research population. According to the Kenya National Bureau of Statistics (KNBs) 2016 MSMEs survey report, Nairobi county has 1,050,600 SMEs. These MSMEs are divided into licensed and unlicensed, with 26 percent (268,100) being licensed and 74 percent (782,500) being unlicensed. Out of the 268,100 licensed MSMEs, 83.8 percent are micro, 14.5 percent are small, and 1.4 percent are medium. Consequently, Nairobi County has 43,539 SMEs that are both registered and licensed.

3.4 Sample Design

Selecting the units of analysis for a study is the process of sampling. It aims to ensure that the findings appropriately reflect the target population (Cooper & Schindler, 2006). This research aims to strike a reasonable compromise between obtaining a sufficient sample size and time and financial restrictions.

Using Cochran's formula with the supposition that 50 percent of the population exhibits the greatest variability (0.5) and a 95 percent confidence level, and a margin of error of 0.07, we obtain:

$n = \frac{Z^2pq}{e^2}$ hence n= $\frac{1.96^2 * 0.5 * (1-0.5)}{0.07^2} = 196$

The participants were chosen using a judgmental sampling. The technique was selected because it is time saving and economical. In this technique, the sample was selected on the basis of available information, intuition or on the basis of the criterion deemed to be self-evident.

3.5 Data Collection

According to Creswell (2002), data collection is the process through which researchers gather information for a study or an investigation. The main source of data for this study was primary data. In order to achieve the research objectives, data was collected using a self-administered structured questionnaire with open- and close-ended questions. There were four parts to the questionnaire i.e., Sections A to D. Section A consisted of general questions about the respondents and their respective organizations, while Sections B, C, and D focused on questions on the extent of BYOD application, motivating factors for BYOD adoption, and information security risks posed by BYOD adoption, respectively. Prior to being given to the respondents, the questionnaires underwent reliability and validity testing.

3.6 Data Analysis

Data analysis is the study of organized information from many perspectives to identify underlying facts. The data to be collected was both qualitative and quantitative in nature. Following completion and collection, the questionnaires were reviewed for completeness and reliability. The data collected was checked for errors and omissions, and the responses were tabulated. To examine the data gathered for this study, descriptive and inferential statistics were applied. As a result, the study used frequencies, percentages, and, when appropriate mean and standard deviation. To evaluate objectives 1, 2 and 3 mean and standard deviation were used. To analyze the association between the extent BYOD adoption and information security risks, a simple linear regression data analysis model was employed.

The analytical model is as follows:

$$Y_{1=}\beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon_1$$

Where:

Y 1 -Information Security Risks

β0- Constant/ Y-intercept

β1, β2, β3, β4- Regression Coefficients, which measure the average change in the value of Y.

X 1 - BYOD use in communication

X 2 - BYOD use in research

X 3 - BYOD use in data management and storage

X 4 - BYOD use in networking

ε1- Error Component

CHAPTER FOUR: DATA ANALYSIS AND RESULTS

4.1 Introduction

The data analysis results are presented in this chapter along with their interpretations. The analysis is founded on the research goal that was to examine the connection between the extent BYOD adoption and information security risks in SMEs in Nairobi County.

4.2 Response Rate

196 respondents were targeted for the study. To ensure that the responses obtained were significant enough, 200 questionnaires were administered but only 115 valid questionnaires were obtained. This represents a 58.67 percent response rate. According to Mugenda and Mugenda (2003), response rate of 50 percent is sufficient, hence the findings of this study can be extrapolated to the population as a whole.

4.3 General Information

4.3.1 Respondent Information

The researcher studied the general information related to the respondents among SMEs based in Nairobi county. They relate to gender, age, education, period of service, type of enterprise, period of operation, sector of the SMEs, number of employees, and annual turnover.

Gender

The respondents were asked to specify their gender. The outcome displays that 64.3 percent were male while 35.7 percent were female.

Table 4.3: Respondents' Gender

	Frequency	Percent	Valid Percent	Cumulative Percent
Male	74	64.35	64.35	64.3
Female	41	35.65	35.65	100.0
Total	115	100.0	100.0	

Age

The respondents were requested to specify their age group. The findings show that the majority of the respondents were younger than 35 years (51.3 percent) while 48.7 percent were above 35 years. This shows that the young generation appreciates the use of technology.

Table 4.4: Respondent's Age

	Frequency	Percent	Valid Percent	Cumulative Percent
25 years or less	23	20.0	20.0	20.0
26 – 35 years	36	31.3	31.3	51.3
36 – 45 years	28	24.3	24.3	75.7
46 – 55 years	12	10.4	10.4	86.1
Over 55 years	16	13.9	13.9	100.0
Total	115	100.0	100.0	

Level of Education

The highest level of education for each respondent was requested. According to the results, 58.3 percent of the respondents said they have a bachelor’s degree, 17.4 percent had masters, 9.6 percent had a certificate, 8.7 percent had diploma while 6.1 percent indicated others like PhD. This reflects an educated workforce within the SME sector in Nairobi where majority possess at least a bachelor’s degree.

Table 4.5: Level of Education

	Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Certificate	10	8.7	8.7	8.7
Diploma	11	9.6	9.6	18.3
Bachelors	67	58.3	58.3	76.5
Masters	20	17.4	17.4	93.9
Other	7	6.1	6.1	100.0
Total	115	100.0	100.0	

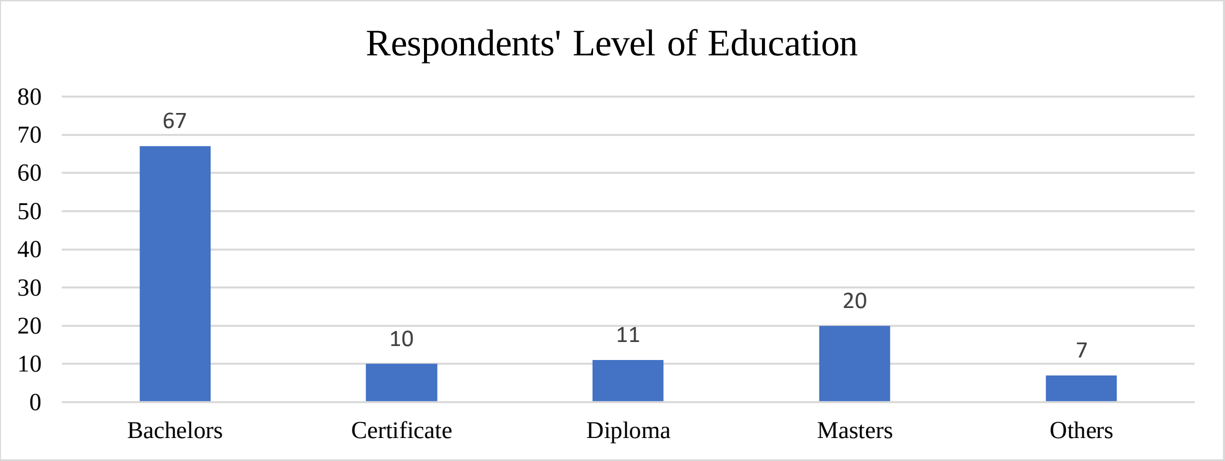

Figure 2- Chart presenting the respondents' level of education

Respondents' Position

The respondents who were chosen for the study all held positions that allowed them to have an extensive understanding of the information technologies adopted by their respective organizations. They were able to articulate and respond to the concerns of the study. Owners, directors, IT administrators, program managers, heads of departments, and supervisors made up the majority of the respondents.

Period of Service

The respondents were requested to indicate how long they had worked with their organization. Their level of experience with the organization was to be indicated by the length of service in the organization. From the outcome, 70.5 percent had been with their employer for more than 5 years thus reflecting that they had a considerable amount of experience with their respective organizations.

Table 4.6: Period of Service

Years	**Frequency**	**Percent**	**Valid Percent**	**Cumulative Percent**
Less than 5	34	29.6	29.6	29.6
5 - 10	30	26.1	26.1	55.7
11 – 15	14	12.2	12.2	67.8
16 – 20	27	23.5	23.5	91.3
More than 20	10	8.7	8.7	100.0
Total	115	100.0	100.0	

4.3.2 Firm Information

Type of Enterprise

A majority of the respondents (68 percent) acknowledged that their firms were partnerships while sole proprietorship and others (limited companies) accounted for 21.7 percent and 31.3 percent, respectively.

Table 4.7: Type of Enterprise

	Frequency	Percent	Valid Percent	Cumulative Percent
Sole Proprietorship	25	21.7	21.7	21.7
Partnership	54	47.0	47.0	68.7
Limited Company	36	31.3	31.3	100.0
Total	115	100.0	100.0	

Years of Business Operation

This question was designed to find out how long the organization has been in existence. The results revealed that 67.83 percent of the sampled SMEs in Nairobi county have been in operation for a period between less than 5 years and 15 years.

Table 4.8: Years of Business Operation

	Frequency	Percent	Valid Percent	Cumulative Percent
Less than 5	34	29.57	29.57	29.57
5 - 10	30	26.09	26.09	55.65
11 - 15	14	12.17	12.17	67.83
16 – 20	27	23.48	23.48	91.30
More than 20	10	8.70	8.70	100.0
Total	115	100.00	100.00	

Organization Category

The respondents were asked to identify a sector of the SMEs that their organizations belonged to. According to the results, 44.3 percent, and 20.0 percent, respectively, of the respondents were from professional services and wholesale and retail trade categories.

Table 4.9: Sector of the SMEs

	Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Financial and Insurance	14	12.2	12.2	12.2
Professional Services	51	44.3	44.3	56.5
Tourism	10	8.7	8.7	65.2
Accommodation and Food Services	10	8.7	8.7	73.9
Wholesale and Retail Trade	23	20.0	20.0	93.9
Other	7	6.1	6.1	100.0
Total	115	100.0	100.0	

Number of Employees

The respondents were requested to state the number of employees that their organization has. A proportion of 68.7 percent had 50 workers and less. This shows that majority of the SMEs sampled are small enterprises. Only 31.3 percent were medium sized.

Table 4.10: Number of Employees

	Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
25 workers or less	52	45.2	45.2	45.2
26 – 50	27	23.5	23.5	68.7
51 – 75	14	12.2	12.2	80.9
76 – 100	4	3.5	3.5	84.3
101 – 125	4	3.5	3.5	87.8
126 – 150	1	.9	.9	88.7
151 – 175	2	1.7	1.7	90.4
Over 175 workers	11	9.6	9.6	100.0
Total	115	100.0	100.0	

Annual Turnover

The approximate annual revenue of the organization in Kenyan shillings was requested from the respondents. Most of the respondents were not willing to provide this information. However, 74 respondents provided an approximate figure and out of these, 66.1 percent (48) quoted amounts between Kshs. 5,000,000.00 and 10,000,000.00 while 33.9 percent quoted values between Kshs. 500,000.00 and 4,900,000.00.

4.4 Extent of BYOD Adoption and Application

The respondents were requested to describe the level of BYOD adoption in their respective organization. This was operationalized by looking at the specific work tasks that employees apply their devices to execute. These tasks were broadly categorized into communication, research, data management and storage, and networking.

4.4.1 Communication

Under communication, the respondents were asked to describe the extent to which they utilized personal gadgets for business communications. The results were tabulated in Table 4.11 below. With an aggregate mean and standard deviation of 3.3304 and 1.4053 respectively, the research findings show that the SMEs in Nairobi County let their employees utilize personal devices for communication to a moderate extent. E-mail correspondence recorded the highest mean (M= 3.4261, SD= 1.5619) among communication related tasks, whereas advertising recorded the lowest mean (M=3.1391, SD=1.2275).

Table 4.11: Extent of BYOD Application in Communication

Tasks	**No Extent**	**Little Extent**	**Moderate Extent**	**Large Extent**	**Very Large Extent**	**Mean**	**Std. Deviation**
	1	**2**	**3**	**4**	**5**		
	Frequency						
E-mail correspondence	25	7	20	20	43	3.4261	1.5619
Voice call	25	0	37	9	44	3.4087	1.5269
Video conferencing	25	7	37	13	33	3.1913	1.4743
Instant messaging	14	10	41	16	34	3.4000	1.3232
Company social media updates	14	9	41	17	34	3.4174	1.3178
Advertising	14	10	64	0	27	3.1391	1.2275
Overall Mean and Standard Deviation						3.3304	1.4053

4.4.2 Research

The respondents were requested to describe the use of personal devices for work related research activities. The results were tabulated in Table 4.12 below. With an aggregate mean and standard deviation at 3.1507 and 1.3039 respectively, the findings showed that SMEs in Nairobi County let employees utilize personal devices for research to a moderate extent. Particularly, preparing presentations and reports recorded the highest mean (M=3.2261, SD=1.3249) while new product development recorded the lowest mean (M=2.0348, SD=1.3241).

Table 4.12: Extent of BYOD Application in Research

Tasks	**No Extent**	**Little Extent**	**Moderate Extent**	**Large Extent**	**Very Large Extent**	**Mean**	**Std. Deviation**
	1	**2**	**3**	**4**	**5**		
	Frequency						
Conducting market research	14	10	61	0	30	3.1913	1.2628
New product development	24	0	65	0	26	2.0348	1.3241
Preparing presentations and reports	14	17	44	9	31	3.2261	1.3249
Overall Mean and Standard Deviation						3.1507	1.3039

4.4.3 Data Management and Storage

The respondents were asked to describe their use of personal devices for data management and storage. The results are shown in Table 4.13 below. With an aggregate mean of 3.0152 and a standard deviation of 1.4426, the research's findings showed that SMEs in Nairobi allowed employees to use personal devices in data management and storage to a moderate extent.

Specifically, storage of corporate data recorded the highest mean (M=3.1739, SD=1.4586) whereas the retrieval of archived files recorded the lowest mean (M=2.8087, SD=1.3370).

Table 4.13: Extent of BYOD Application in Data Management and Storage

Tasks	**No Extent**	**Little Extent**	**Moderate Extent**	**Large Extent**	**Very Large Extent**	**Mean**	**Std. Deviation**
	1	**2**	**3**	**4**	**5**		
	Frequency						
Storing corporate data	24	11	31	19	30	3.1739	1.4586
Customer database maintenance	28	9	45	0	33	3.0087	1.4897
Retrieval of archived files	24	20	48	0	23	2.8087	1.3370
Data entry	24	17	34	7	33	3.0696	1.4851
Overall Mean and Standard Deviation						3.0152	1.4426

4.4.4 Networking

According to the respondents, organizations allowed employees to use personal devices in networking to a moderate extent with an aggregate mean of 3.1913 and a standard deviation of 1.3792. The findings indicate that SMEs in Nairobi allow their employees to use their devices to a moderate extent in accessing company applications thus recording the highest mean (M= 3.3043, SD=1.3057). Following closely is in accessing office emails (M= 3.2696, SD=1.3267). The results are shown in Table 4.14.

Table 4.14: Extent of BYOD Application in Networking

Tasks	**No Extent**	**Little Extent**	**Moderate Extent**	**Large Extent**	**Very Large Extent**	**Mean**	**Std. Deviation**
	1	**2**	**3**	**4**	**5**		
	Frequency						
Share and transfer of files	24	10	41	7	33	3.1304	1.4601
Accessing the corporate network	24	54	0	14	23	3.1043	1.3270
Accessing office e-mails	14	14	47	7	33	3.2696	1.3267
Accessing company applications	14	10	51	7	33	3.3043	1.3057
Accessing company IT support	28	0	47	7	33	3.1478	1.4764
Overall Mean and Standard Deviation						3.1913	1.3792

The findings suggest that SMEs have adopted BYOD to a moderate extent. Employees are allowed to use their devices in executing their contractual obligations across all the categories with the extent of BYOD application in communication recording the highest mean (M= 3.3304, SD=1.4053).

4.5 Motivating Factors for BYOD Adoption

One of the objectives of the study was to determine what factors encouraged SMEs in Nairobi to use BYOD in the workplace. The need to increase employee mobility stood out as biggest motivating factor (M=3.2348, SD=1.4469) whereas the need to reduce the maintenance and device upkeep costs (M=2.7217, SD=1.3282) and to keep up with technology development (M=2.7217, SD=1.2393) had the least influence on the adoption of BYOD among SMEs in Nairobi.

Table 4.15: Motivating Factors for BYOD Adoption

Motivating Factors	**No Extent**	**Little Extent**	**Moderate Extent**	**Large Extent**	**Very Large Extent**	**Mean**	**Std. Deviation**
	1	**2**	**3**	**4**	**5**		
	Frequency						
Need to enhance employee productivity and efficiency	21	32	24	10	28	2.9304	1.4432
Need to improve employee mobility	25	10	17	39	24	3.2348	1.4469
Need to foster collaboration as a result of remote and hybrid work	25	0	49	30	11	3.0174	1.2353
Need to reduce the time and costs associated with training employees to use new technology	35	0	42	21	17	2.8696	1.4112
Need to save on the cost of hiring IT support teams	25	0	51	23	16	3.0435	1.2800
Need to reduce the maintenance and device upkeep costs	25	27	37	7	19	2.7217	1.3282
Need to keep up with technology development.	25	23	36	21	10	2.7217	1.2393
Need to gain a competitive advantage	21	27	36	10	21	2.8522	1.3327

4.6 Information Security Risks and BYOD Adoption

The research sought to find out the information security risks that have actually been experienced as a result of the adoption of BYOD. The majority of respondents felt that data leakage has been experienced to a large extent, as indicated by the highest mean of 4.0696 with a standard deviation of 0.9526. Targeted attacks recorded the lowest mean (M=2.2174) indicating that this risk had been experienced to a little extent.

Table 4.16: Information security risks and BYOD Adoption

Information Security Risks	**No Extent**	**Little Extent**	**Moderate Extent**	**Large Extent**	**Very Large Extent**	**Mean**	**Std. Deviation**
	1	**2**	**3**	**4**	**5**		
	Frequency						
Data leakage	2	7	15	48	43	4.0696	0.9526
Virus infection	12	28	32	25	18	3.0783	1.2294
Spyware infection	16	21	29	26	23	3.1652	1.3241
Identity theft	32	23	23	23	14	2.6870	1.3852
Phishing	28	18	24	25	20	2.9217	1.4336
Targeted attacks	47	25	20	17	6	2.2174	1.2689
Data interception	25	30	14	28	18	2.8609	1.4135
Loss/theft of devices	2	4	20	56	33	3.9913	0.8735
Insider threats	13	12	33	29	28	3.4087	1.2766
User policy violations	20	27	28	16	24	2.9739	1.3858

4.7 Regression Analysis

Table 4.17: Model Summary

Goodness of Fit Statistics (Y)	
Multiple R	0.1924
R Square	0.0370
Adjusted R Square	0.0020
Standard Error	0.4728
Observations	115

The correlation coefficient (Multiple R) of 0.1924 suggests a weak positive linear relationship between the two variables. The model can be partially used to predict information system risks. This was shown by a coefficient of determination (R) of 0.0370 thus suggesting there is little correlation between the two variables if any.

To examine the relationship between BYOD adoption and information security risk in SMEs in Nairobi county, variance analysis was appropriate. The variables were regressed at 95% confidence interval level.

Table 4.18: ANOVA

ANOVA					
	Df	SS	MS	F	Significance F
Model	4	0.9447	0.2362	1.0568	0.3815
Error	110	24.5845	0.2235		
Corrected	114	25.5292			

The computed p-value exceeds the significance level α=0.05. This means that the sample data does not provide sufficient evidence to conclude that the regression model fits the data better than the model with no independent variables.

Table 4.19: Roy's test

	X1	**X2**	**X3**	**X4**
Lambda	0.899	0.986	0.000	0.000
F Observed values	1.453	0.471	0.000	0.000
DF1	8	3	0	0
DF2	103	103	0	0
F Critical value	2.030	2.693	0.000	0.000
p-value	0.184	0.703	**<0.0001**	**<0.0001**

H0: The variable or the interaction of the corresponding column has no significant effect on the dependent variable.

Ha: The variable or the interaction of the corresponding column has a significant effect on the dependent variable.

X1: As the computed p-value is greater than the significance level α=0.05, one cannot reject the null hypothesis. The risk to reject the null hypothesis H0 while it is true is 18.36%.

X2: As the computed p-value is greater than the significance level α=0.05, one cannot reject the null hypothesis. The risk to reject the null hypothesis H0 while it is true is 70.31%.

X3: As the computed p-value is lower than the significance level α=0.05, one should reject the null hypothesis and accept the alternative hypothesis, Ha. The risk to reject the null hypothesis H0 while it is true is lower than 0.01%.

X4: As the computed p-value is lower than the significance level α=0.05, one should reject the null hypothesis and accept the alternative hypothesis, Ha. The risk to reject the null hypothesis H0 while it is true is lower than 0.01%.

Table 4.20: Coefficients

	Coefficients	**Std Error**	**t Stat**	**P-value**	**Lower 95%**	**Upper 95%**
Intercept	3.2784	0.1365	24.0113	0.0000	3.0078	3.5489
X1	-0.0040	0.0806	-0.0490	0.9610	-0.1637	0.1558
X2	-0.0869	0.0546	-1.5911	0.1145	-0.1952	0.0213
X3	0.1213	0.2218	0.5467	0.5857	-0.3184	0.5609
X4	-0.0688	0.2621	-0.2626	0.7934	-0.5882	0.4506

The expected information security risks, with all the predictor variables held constant, are estimated to be 3.2784 based on the calculated Y-intercept. We can see that the independent variables (p-values 0.9610, 0.1145, 0.5857 and 0.7934, respectively) are not statistically significant. Therefore, the following estimated regression equation was created using these coefficients from the model’s output:

$$Y= 3.278- 0.004X_1- 0.087X_2 + 0.121X_3 -0.069X_4$$

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary of the results and draws conclusions from them in light of the research objectives.

5.2 Summary of the Findings

The main research objective was to assess the relationship between BYOD adoption and information security risks in SMEs in Nairobi County. The study specifically attempted to establish the extent of BYOD application in SMEs; determine the drivers for BYOD adoption; and establish the connection between BYOD adoption and information security risks in SMEs in Nairobi County. On the extent of BYOD application in SMEs, the study looked at the extent to which the employees were allowed to use personal devices in executing their contractual duties. These tasks were broadly categorized into four namely communication, research, data management and storage, and networking. The results indicate that the SMEs have adopted BYOD to a moderate extent across all the categories of tasks, with communication recording the highest mean.

The study also aimed at identifying the drivers for BYOD adoption. The need to increase employee mobility, save on the costs of hiring IT, foster collaboration as a result of remote and hybrid work, to enhance employee productivity and efficiency were the main drivers of BYOD adoption, as per the data collected. Thus, proving that BYOD adoption in the context of SMEs is out of necessity.

On the information security risks brought about by BYOD adoption, the study found out that data leakage has been experienced to a large extent, and loss/theft of employees' personal devices used in BYOD, insider threats, spyware and virus infections had been experienced at a moderate extent. Identity theft, phishing, targeted attacks, data communication interception, and user policy violations had been experienced to a little extent.

The regression analysis summary showed that the extent of BYOD adoption and application in communication, research and networking have a negative relationship with information security risks. A unit increase in communication, research and networking would reduce information security risks by 0.0040, 0.0869, and 0.0688, respectively. Data management and storage has a positive relationship with information risks. A unit increase in data management and storage results in an increase in information security risks by 0.1213.

5.3 Conclusions of the Study

The purpose of this research was to report on the relationship between BYOD adoption and information security risks in SMEs based in Nairobi County. The findings show that although BYOD has been adopted to a moderate extent, it is still yet to be appreciated as a concept in SMEs in Nairobi. Given the responses, it is evident that the trend is there and as such the SMEs have adopted it as an alternative means of improving employee mobility, productivity, and efficiency, to save on the cost of hiring IT support teams, and to foster collaboration as a result of remote and hybrid work. The contribution of this research thus, demonstrates that the SMEs use BYOD as a necessity to fulfil organizational job duties.

On the information security risks experienced as a result of BYOD adoption, data leakage and loss/theft of devices used for BYOD were highly ranked as having been experienced to a large extent. Insider threats and malware were also cited as information security risks that have been experienced to a moderate extent while user policy violations, identity theft, phishing, targeted attacks, and data communication interception have been experienced to a little to no extent at all. However, the regression model suggests that there is little, if any correlation between the extent of BYOD adoption and application in communication, research, data management and storage, and networking and information security risks. This suggests that there is little or no evidence that the occurrence of information security risks is related with the extent of BYOD adoption among SMEs in Nairobi County. This presents a productivity paradox because with BYOD adoption we would expect the information security risks to go up and not down.

5.4 Recommendations of the Study

The research confirms that BYOD has taken roots in SMEs in Nairobi County. Therefore, there is need to sensitize the top-level management on the phenomenon to appreciate it as a formal concept and fully understand the risks it poses before adoption. Additionally, educational programs should be created to enlighten the employees.

5.5 Limitations of the Study

Despite the study’s valuable findings, there were shortcomings. First, I had to rely on research assistants to help me gather data. Their training and the activity of data collection was time consuming and costly. Second, the time available for the study was limited due to the deadlines set for the submission of the report. Third, a larger sample size may have led to more accurate results considering the number of registered and licensed SMEs based in Nairobi County. Fourth, the study’s descriptive cross-sectional design could only provide a snapshot of the process because the extent of BYOD adoption is a dynamic occurrence. Therefore, it is conceivable that the current BYOD adoption extent in SMEs could change, and this will invalidate the results of this study at a later time.

5.6 Areas Suggested for Future Research

This study recommends additional research on the elements that contribute to successful BYOD adoption and implementation among Kenyan SMEs. Additionally, researchers should explore the security countermeasures to address information security risks and threats through BYOD adoption in the same context.

REFERENCES

Agarwal, R., & Prasad, J. (1998). A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology. *Information Systems Research*, *9*(2), 204-215. doi: 10.1287/isre.9.2.204.

Akin-Adetoro, A., & Kabanda, S. (2021). Factors affecting the adoption of BYOD in South African small and medium enterprise s. *The Electronic Journal Of Information Systems In Developing Countries*, *87*(6). doi: 10.1002/isd2.12185.

Alcatel- Lucent. (2013). *Kindsight Security Labs Malware Report – Q4 2013* (p. 5). Alcatel- Lucent. Retrieved from http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9861-kindsight-security-labs-malware-report-q4-2013.pdf.

Arwa, J. (2014). Adoption of Bring Your Own Device to Enhance Customer Service Delivery in Kenya Commercial Bank (Masters). University of Nairobi.

Ayyagari, R., & Figueroa, N. (2017). Is Seeing Believing? Training Users on Information Security: Evidence from Java Applets. *Journal Of Information Systems Education*, *28*(2), 115-122. Retrieved 30 July 2022.

Baillette, P., & Barlette, Y. (2018). BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs. *Journal Of Organizational Change Management*, *31*(4), 839-851. doi: 10.1108/jocm-03-2017-0044.

Bagozzi, R. (2007). The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. *Journal Of The Association For Information Systems*, *8*(4), 244-254. doi: 10.17705/1jais.00122.

Baker, J. (2011). The Technology–Organization–Environment Framework. *Information Systems Theory*, *28*, 231-245. doi: 10.1007/978-1-4419-6108-2_12.

Bello, A., Murray, D., & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information &Amp; Computer Security*, *25*(4), 475-492. https://doi.org/10.1108/ics-03-2016-0025.

Boateng, E., & Boaten, F. (2016). Bring-Your-Own-Device (BYOD): An Evaluation of Associated Risks to Corporate Information Security. *International Journal Of Information Technology (IT) & Engineering*, *4*(8), 12-30. Retrieved 30 July 2022.

Business Daily. (2021). Rwanda jails 8 Kenyans in Equity Bank hacking case. Retrieved from https://www.businessdailyafrica.com/bd/economy/rwanda-jails-8-kenyans-equity-bank-hacking-case-3463792.

Carranza, H., Carranza, A., & Zaidi, S. (2019). Bring Your Own Device (BYOD) Also Brings New Security Challenges. *World Congress On Electrical Engineering And Computer Systems And Science*. doi: 10.11159/cist19.116.

Chau, P., & Hu, P. (2002). Examining a Model of Information Technology Acceptance by Individual Professionals: An Exploratory Study. *Journal Of Management Information Systems*, *18*(4), 191-229. doi: 10.1080/07421222.2002.11045699.

Cilliers, L. (2019). Wearable devices in healthcare: Privacy and information security issues. *Health Information Management Journal*, *49*(2-3), 150-156. https://doi.org/10.1177/1833358319851684.

Cisco Systems Inc. (2012). *Cisco Systems Inc.,2012 Annual Report*. Washington D.C: Cisco Systems Inc.

Cooper, D., & Schindler, P. (2014). *Business Research Methods* (12th ed.). New York: McGraw-Hill/Irwin.

Creswell, J. (2002). Educational research: Planning, conducting, and evaluating Quantitative and Qualitative research. Upper Saddle River, NJ: Merrill Prentice Hall.

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers &Amp; Security*, *32*, 90-101. https://doi.org/10.1016/j.cose.2012.09.010.

Da Veiga, A., Astakhova, L., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers &Amp; Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713.

Davis, F., Bagozzi, R., & Warshaw, P. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, *35*(8), 982-1003. doi: 10.1287/mnsc.35.8.982.

DeHayes, D., Hoffer, J., Martin, E., &amp; Perkins, W. (2014). Managing information technology (7th ed.). Harlow, Essex: Pearson.

Deloitte Kenya. (2016). Deloitte Kenya Economic Outlook Report. Deloitte.

Development of Bring-Your-Own-Device Risk Management Model: A Case Study from a South African Organisation Ivan Veljkovic and Adheesh Budree.

Doargajudhur, M., & Dell, P. (2018). The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation. *Journal Of Computer Information Systems*, *60*(6), 518-529. https://doi.org/10.1080/08874417.2018.1543001.

Evans, D. (2022). What is BYOD and why is it important? [Blog]. Retrieved from https://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important-1175088.

Evripidis, R. (2008). Lawful Interception and Countermeasures- In the Era of Internet Telephony (Ph. D). Royal Institute of Technology.

Forrester (2012). Mobile Workers user Personal Apps to Solve Customer Problems – Is It Ready, Willing, And Able to Assist? A Forrester Consulting Thought Leadership Paper commissioned by Unisys.

French, A., Guo, C., & Shim, J. (2014). Current Status, Issues, and Future of Bring Your Own Device (BYOD). *Communications Of The Association For Information Systems*, *35*. doi: 10.17705/1cais.03510.

Gantz, S., Philpott, D., & Windham, D. (2013). *FISMA and the risk management framework* (1st ed.). Amsterdam: Elsevier/Syngress.

Garba, A., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments. *Journal Of Information Privacy And Security*, *11*(1), 38-54. doi: 10.1080/15536548.2015.1010985.

Harris, J., Ives, B., &amp; Junglas, I. (2012). IT Consumerization: When Gadgets Turn into Enterprise IT Tools. AIS Library, 11(3), 99-112.

Kabanda, S., & Brown, I. (2014). Bring-Your-Own-Device (BYOD) practices in SMEs in Developing Countries – The Case of Tanzania. In *25th Australasian Conference on Information Systems*. New Zealand: ACIS.

Kamau, W. (2013). The Bring Your Own Device Phenomena: Balancing Productivity and Corporate Data Security (Masters). University of Nairobi.

Kenya - Information, Communications and Technology (ICT). (2021). Retrieved 6 August 2022, from https://www.trade.gov/country-commercial-guides/kenya-information-communications-and-technology-ict.

Kenya National Bureau of Statistics. (2016). *Micro, Small and Medium Establishment (MSME) Survey* (pp. 31-35). Nairobi: Kenya National Bureau of Statistics.

Kimatu, S. (2021). Kenya: 300 Stolen Phones Recovered, Two Seized in Sting Operation. *Daily Nation*.

Kitten, T. (2013). Was Citi Breach Preventable? [Blog]. Retrieved from https://www.bankinfosecurity.com/was-citi-breach-preventable-a-6042

Kohlios, C., & Hayajneh, T. (2018). A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. *Electronics*, *7*(11), 284. do: 10.3390/electronics7110284.

Kutoto, J. (2020). Adoption of "Bring Your Own Device" at the Workplace by Non- Governmental Organizations in Kisumu County, Kenya (Masters). University of Nairobi.

Lai, V., & Guynes, J. (1997). An Assessment of the Influence of Organizational Characteristics on Information Technology Adoption Decision: A Discriminative Approach. *IEEE Transactions On Engineering Management*, *44*(2), 146-157. doi: 10.1109/17.584923.

Leavitt N. (2013) 'Today's mobile security requires a new approach'. IEEE Computer Society, 46: pp. 16-19.

Lee, J., Warkentin, M., Crossler, R., & Otondo, R. (2016). Implications of Monitoring Mechanisms on Bring Your Own Device Adoption. *Journal Of Computer Information Systems*, *57*(4), 309-318. https://doi.org/10.1080/08874417.2016.1184032.

Lee, M., & Cheung, C. (2004). Internet Retailing Adoption by Small-to-Medium Sized Enterprises (SMEs): A Multiple-Case Study. *Information Systems Frontiers*, *6*(4), 385-397. doi: 10.1023/b: isfi.0000046379.58029.54.

Li, L., & Lin, T. (2019). Smartphones at Work: A Qualitative Exploration of Psychological Antecedents and Impacts of Work-Related Smartphone Dependency. *International Journal Of Qualitative Methods*, *18*, 160940691882224. doi: 10.1177/1609406918822240.

Loose, M., Weeger, A., & Gewald, H. (2013). BYOD–the next big thing in recruiting? Examining the determinants of BYOD service adoption behavior from the perspective of future employees.

Lyndon, E. (2014). The Benefits and Threats of BYOD in a SME Enterprise: A Systematic Literature Review (Masters). Lulea University of Technology.

Lyytinen, K., & Damsgaard, J. (2001). What's Wrong with the Diffusion of Innovation Theory? *Diffusing Software Product And Process Innovations*, 173-190. doi: 10.1007/978-0-387-35404-0_11.

Mbalanya, M. (2013). Bring Your Own Device and Corporate Information Technology Security: Case of Firms Listed in the Nairobi Stocks Exchange (Masters). University of Nairobi.

Miller-Merrell, J. (2012). The workplace engagement economy where HR, social, mobile, and tech collide. *Employment Relations Today*, *39*(2), 1-9. doi: 10.1002/ert.21359.

Mordor Intelligence. (2020). *Bring-Your-Own-Device (BYOD) Market – Growth, Trends, Covid-19 Impact, and Forecasts (2021 – 2026)*. Telangana, India: **Mordor Intelligence**.

Moschella D, Neal D, Opperman P and Taylor J (2004). The Consumerization of IT. CSC's Research &amp; Advisory Services Position Paper.

Mputhia, C. (2020). Why Kenya needs a standalone SMEs law. *Business Daily*.

Mutegi, C. (2015, November). Jua Kali Sector Plays Key Role in Economic Development and Job Creation. Retrieved August 08, 2022, from http://www.mygov.go.ke/smes-play-key-role-ineconomic-development-and-job-creation.

Mugenda, O. M., & Mugenda, A. G. (2003). Research methods: Quantitative and qualitative approaches. Nairobi, Kenya: African Centre for Technology Studies.

Mwanzau, R.W. (2014). Motivation for consumerization of information technology (COIT): an investigation of knowledge workers in the road sector in Kenya.

Nabila, A. (2014). *The Impact of Cyber Security on SMEs* (Maters). University of Twente.

Namunwa, K. (2021). Kenyan SMEs Suffering the Most From Cyber Security Threats. Retrieved 6 August 2022, from https://cioafrica.co/kenyan-smes-suffering-the-most-from-cyber-security-threats.

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). An introduction to information security. https://doi.org/10.6028/nist.sp.800-12r1.

Obote, V. (2019). Identity and Authentication Model for Bring Your Own Device in Organizations (Masters). University of Nairobi.

Ogie, R. (2016). Bring Your Own Device: An overview of risk assessment. *IEEE Consumer Electronics Magazine*, *5*(1), 114-119. doi: 10.1109/mce.2015.2484858.

Oliver R. (2012). Why the BYOD Boom is Changing How We Think About Business IT. *E and T Magazine, November 2012 Issue*.

Oonge, S., Muhambe, M., & Ratemo, C. (2021). A Bring Your Own Device Risk Assessment Model. *International Journal Of Security (IJS), 12*(2).

Ophoff, J., & Miller, S. (2019). Business Priorities Driving BYOD Adoption: A Case Study of a South African Financial Services Organization. *Issues In Informing Science And Information Technology*, *16*, 165-196. doi: 10.28945/4303.

Ounza, J., Liyala, S., & Ogara, S. (2018). Emerging Security Challenges due to Bring Your Own Device Adoption: A Survey of Universities in Kenya. *International Journal Of Science And Research*, *7*(1), 345-348. Retrieved 30 July 2022.

Owl Labs. (2021). State of Remote Work- 5th Annual Edition.

Pemarathna, R. (2020). Does Bring Your Own Device (BYOD) Adoption Impact on Work Performance? *Does Bring Your Own Device (BYOD) Adoption Impact On Work Performance? IV* (1), 242-244.

Pham, D., Pittayachawan, S., Bruno, V., &amp; Kautz, K. (2019). Investigating the diffusion of IT consumerization in the workplace: A case study using social network analysis. Information System Frontiers, 21, 941-955.

Pitichat, T. (2013). Smartphones in the workplace: Changing organizational behavior, transforming the future. *LUX*, *3*(1), 1-10. doi: 10.5642/lux.201303.13.

Rogers, E. (2003). *Diffusion of innovations* (5th ed.). Simon and Schuster.

Sadiku, M.N.O., Nelatury, S.R. and Musa, S.M. (2017). Bring your own device. Journal of Scientific and Engineering Research, 4 (4), 163-165.

Sánchez-Franco, M., & Roldán, J. (2005). Web acceptance and usage model. *Internet Research*, *15*(1), 21-48. doi: 10.1108/10662240510577059.

Serianu (2014). Rethinking Cyber Security – An Integrated Approach: Processes, Intelligence and Monitoring. Kenya Cyber Security Report 2014.

Serianu Ltd. (2015). *Kenya Cyber Security Report 2015* (p. 12). Nairobi: Serianu Ltd.

Siddiqui, R. (2014). Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges. *International Journal Of Emerging Trends & Technology In Computer Science*, *3*(1), 233-236.

Shondo, F. (2019). Bring Your Own Device Phenomenon and Information Security at Jaramogi Oginga Odinga Teaching and Referral Hospital in Kisumu County, Kenya. (Masters). University of Nairobi.

Soomro, Z., Shah, M., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal Of Information Management*, *36*(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009.

Symantec. (2016). *Internet Security Threat Report* (p. 7). Symantec.

Talabis, M., & Martin, J. (2013). *Information security risk assessment toolkit*. Amsterdam: Elsevier.

Tornatzky, L., Fleischer, M., & Chakrabarti, A. (1990). *The processes of technological innovation* (1st ed.). Lexington, Mass.: Lexington Books.

Tromp, L. A. D., & Kombo, K. D. (2006). Proposal and thesis writing. An Introduction, University Education Book service University Press version) Industrial and labor relations review, 55, 3-21.

Unisys. 2010. Unisys Consumerization of IT Benchmark Study. Blue Bell, Pennsylvania, USA.

Van Raaij, E., & Schepers, J. (2008). The acceptance and use of a virtual learning environment in China. *Computers &Amp; Education*, *50*(3), 838-852. doi: 10.1016/j.compedu.2006.09.00.1.

Venkatesh, V., & Davis, F. (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.

Venkatesh, V., & Zhang, X. (2010). Unified Theory of Acceptance and Use of Technology: U.S. Vs. China. *Journal Of Global Information Technology Management*, *13*(1), 5-27. doi: 10.1080/1097198x.2010.10856507.

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425. doi: 10.2307/30036540.

Wangutusi, G. (2015). An Exploration of How BYOD (Bring Your Own Device) User Behavior Impacts on an Organization’s Information Security: A Case Study of Madison Insurance Company Kenya Limited (Masters). University of Nairobi.

WatchGuard (2013). Ten Tips for Establishing a Secure Foundation for BYOD. WatchGuard Technologies Whitepaper, 2-7.

Weiß, F., & Leimeister, J. (2012). Consumerization. *WIRTSCHAFTSINFORMATIK*, *54*(6), 351-354. doi: 10.1007/s11576-012-0338-y.

APPENDIX 1: Questionnaire

INSTRUCTIONS

This questionnaire seeks to collect information on BYOD Adoption and Information Security Risks among Small and Medium Enterprises in Nairobi County. Please provide information in the spaces provided by filling appropriately.

SECTION A: GENERAL INFORMATION

RESPONDENT INFORMATION

1. **Indicate your gender.**
   Male [ ]   Female [ ]

2. **What age bracket do you fall under?**
   25 years or less   [ ]
   26 – 35 years   [ ]
   36 – 45 years   [ ]
   46 – 55 years   [ ]
   Over 55 years   [ ]

3. **Please indicate your highest level of education.**

   Certificate [ ]   Diploma [ ]   Bachelors [ ]   Masters [ ]

Other (please specify) …………………………………

4. **What is your position within the organization?**
   ………………………………………………………..

3. **How long have you worked for the organization (in years)?**

Less than 5	
5 - 10	
11 – 15	
16 - 20	
More than 20	

FIRM INFORMATION

5. **What kind of an enterprise is the organization?**

Sole Proprietorship	Partnership

Other (please specify):……………………

6. **How long has the organization been in operation (in years)?**

Less than 5	
5 - 10	
11 – 15	
16 - 20	
More than 20	

7. **To what sector of the SMEs does the organization belong?**

Financial and Insurance	
Professional Services	
Manufacturing	
Tourism	
Arts, Entertainment and Recreation	
Accommodation and Food Services	
Wholesale and Retail Trade	
Other (Please specify)	

8. How many employees does the organization have?

25 workers or less	
26 – 50	
51 – 75	
76 – 100	
101 – 125	
126 – 150	
151 - 175	
Over 176 workers	

9. What is the approximate annual turnover of the organization in Kshs?

…………………………………………………………………………………

SECTION B: EXTENT OF BYOD ADOPTION

10. **To what extent does the organization allow employees to use personal mobile devices for the following tasks of the organization at the workplace?** *Please indicate the extent using the scale provided.*
1 = No extent at all; 2= Little extent; 3= Moderate extent;
4= Large extent; 5= Very large extent.

Application	**No extent at all (1)**	**Little extent (2)**	**Moderate extent (3)**	**Large extent (4)**	**Very large extent (5)**
Communication					
E-mail correspondence					
Voice calls					
Video conferencing					
Instant messaging					
Company social media updates					
Advertising					
Research					
Conducting market research					
New product development					
Preparing presentations and reports					
Data Management and Storage					
Storing corporate data					
Customer database maintenance					
Retrieval of archived files					
Data entry					
Networking					
Share and transfer of files					
Accessing the corporate network					
Accessing office e-mails					
Accessing company applications					
Accessing company IT support					
Others, specify and rate accordingly					

SECTION C: MOTIVATING FACTORS FOR BYOD ADOPTION

11. **To what extent was each of the following a motivating factor in allowing employees to use their personal mobile devices for the organization work?** *Please indicate the extent in the scale provided*.

1 = No extent at all; 2= Little extent; 3= Moderate extent; 4= Large extent; 5= Very large extent.

Motivating Factors	**No extent at all (1)**	**Little extent (2)**	**Moderate extent (3)**	**Large extent (4)**	**Very large extent (5)**
Need to enhance employee productivity and efficiency					
Need to improve employee mobility					
Need to foster collaboration as a result of remote and hybrid work					
Need to reduce the time and costs associated with training employees to use new technology					
Need to save on the cost of hiring IT support teams					
Need to reduce the maintenance and device upkeep costs.					
Need to keep up with technology development.					
Need to gain a competitive advantage.					
Others, specify and rate accordingly					

SECTION D: INFORMATION SECURITY RISKS AND BYOD ADOPTION

12. **To what extent has the organization experienced each of the following information security risks as a result of allowing employees to use personal mobile devices for the organization work?** *Please indicate the extent in the scale provided*.

1 = No extent at all; 2= Little extent; 3= Moderate extent;
4= Large extent; 5= Very large extent.

Information security risks and BYOD Adoption	**No extent at all (1)**	**Little extent (2)**	**Moderate extent (3)**	**Large extent (4)**	**Very large extent (5)**
Data leakage (access of corporate data from within the organization by external parties)					
Virus infection (A virus is a malicious software program loaded onto a user's computer without their knowledge and performs malicious actions)					
Spyware infection (Spyware is a malicious software installed on a computing device without the end user's knowledge to gather the user's data and relay it to a third party without the user's consent)					
Identity theft (Situation where log-in credentials are stolen and used to access system for fraudulent purposes)					
Phishing (Phishing is when attackers send malicious emails designed to trick people into falling for a scam)					
Targeted attacks (A malicious attack perpetrators actively pursue and compromise an organization's infrastructure)					
Data communication interception (An attack against confidentiality where perpetrators access non-public transmission of data to, from or within the organization's network)					
Loss/theft of devices used in BYOD leading to vulnerability of the organization's information system.					
Insider threats (insider uses their authorized access wittingly or unwittingly to do harm to the security of an organization's operations or assets)					
User policy violations (users disabling anti-virus and firewall applications and/or accessing and downloading content from untrusted websites)					
Others, specify and rate accordingly					

THANK YOU FOR YOUR TIME!

APPENDIX 2: Introduction Letter

UNIVERSITY OF NAIROBI

FACULTY OF BUSINESS AND MANAGEMENT SCIENCES

OFFICE OF THE DEAN

Telegrams: "Varsity",
Telephone: 020 491 0000
VOIP: 9007/9008
Mobile: 254-724-200311

P.O. Box 30197-00100, G.P.O.
Nairobi, Kenya
Email: *fob-graduatestudents@uonbi.ac.ke*
Website: ***business.uonbi.ac.ke***

Our Ref: **D61/13450/2018** November 09, 2022

National Commission for Science, Technology and Innovation

NACOSTI Headquarters

Upper Kabete, Off Waiyaki Way

P. O. Box 30623- 00100

NAIROBI

RE: INTRODUCTION LETTER: JANET WALI MWAWALI

The above named is a registered Masters of Business Administration candidate at the University of Nairobi, Faculty of Business and Management Sciences. She is conducting research on ***"Bring Your Own Device Adoption and Information Security Risks Among SMEs in Nairobi County."***

The purpose of this letter is to kindly request you to assist and facilitate the student with necessary data which forms an integral part of the Project.

The information and data required is needed for academic purposes only and will be treated in **Strict-Confidence**.

Your co-operation will be highly appreciated.

Dean's Office
University of Nairobi
Faculty of Business
and Management Science
P O Box 30197-00100, Nairobi

PROF. JAMES NJIHIA

DEAN, FACULTY OF BUSINESS AND MANAGEMENT SCIENCES