**UNIVERSITY OF NAIROBI**

**SCHOOL OF COMPUTING AND INFORMATICS**

# 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

**Submitted by**

**Gerald Nyamaiko Mutoro Wangutusi**

**P56/61482/2013**

**Supervisor**

**Mr. Samuel Ruhiu**

**Submitted in partial fulfillment of the requirements of the Master of Science in Information Systems**

**DECLARATION**

I declare that this thesis is my original work and has never been submitted to any other University or institution of higher learning for examination. The thesis is a result of my own individual effort and where other people's ideas and work have been cited, they are acknowledged.

Signature:_____ Date:_____

Wangutusi, Gerald Mutoro Nyamaiko

P56/61482/2013

This research thesis has been submitted for examination with my approval as the University supervisor.

Signature: _____ Date: _____

Mr. Samuel Ruhiu

## PREFACE

I would like to take this opportunity to acknowledge how this Master of Science in Information Systems course has not only positively changed me but has also enriched by professional stance with regard to the challenges that face the both public and private business sectors in Kenya.

The knowledge attained from this postgraduate course has been intensely practical and as such, I am certain that it will augment my contribution to the public and public sectors that I am so proud to serve.

## DEDICATION

This work is dedicated to my dear wife Serah W. Mungai who was always there for me during the most difficult times, with tireless support and infinite encouragement during my entire MSc. course. My daughter Shanice and son Maurice for their support, prayers and sacrifice, my mum Eunice Wangutusi and dad Maurice Wangutusi who have actually made me who I am and taught me the value of education and hard work.

My dedication also goes to my sisters. Thank you all for the support and encouragement you accorded me.

Finally, my dedication goes to my supervisor Mr. Samuel Ruhiu who was always available to discuss my work and made tremendous sacrifices in ensuring my thesis was of high quality. Tremendous gratitude also goes to my MSc. (IS) Panel; Professor Elijah Omwenga, Professor Peter W. Wagacha and Dr. Evans Miriti for their dedication and sacrifice in creating time to guide this research.

To all of you, thank you.

## ABSTRACT

This research explores how BYOD (Bring Your Own Device) user behavior impacts on an organization's information security, a case study of Madison Insurance Company Kenya Limited (MICK). An empirical survey, using two (2) different sets of self administered questionnaires was conducted to achieve this purpose; the random sample questionnaire (hand-delivered) and the expert sample questionnaire (through email).

Every MICK branch approximately has four (4) units, making a total of eighty-four (84) units. The researcher randomly singled out four (4) employees per a branch to create a total of eighty-four (84) respondents who gave their feedback through questionnaires. The rationale behind this choice was to have representation from each and every MICK branch.

The expert sample respondents were specific because the survey inquiry required those with specialized knowledge to give their opinions. As such, the sample identified for this purpose comprised entirely of the ICT department staff.

The results of this research revealed that majority of the BYOD users do actually engage in certain behaviors that put informational assets in portable devices (BYODs) at risk. However, the level of risky behavior was not found to be as high as anticipated. More so, a commendable degree of user knowledge on information security existed and consequently the threats/vulnerabilities posed to the company were found to be considerably low. It was however inferred that a high likelihood of an influx of user owned devices into the work place was greatly probable hence a foreseeable growth in data and information security threats.

This research's results thus enable MICK to better understand the dynamics of user behavior and hence aid in facilitation and implementation of BYOD policies that factor-in these behaviors and consequently foster a safer and more secure BYOD ICT environment. The adoption of a befitting BYOD model for the company was thus recommended since the environment at MICK was deemed ripe for such.

In order to achieve this, the optimized hybrid conceptual framework for BYOD adoption in particular was developed as a model befitting the MICK BYOD scenario. The attractiveness of this model and its agreeability with the study findings was its flexibility and the fact that it took into consideration the underlying organizational infrastructure. Therefore, its implementation will have positive implications on the MICK's BYOD policy formulation moving forward.

## ACKNOWLEDGEMENT

Many thanks to God, the Almighty, who made it possible for me to finish my MSc. degree. Sincere thanks to my boss Mr. James O. Nyakomitta for granting me leave whenever it was necessary to study and sit for my exams.

I also wish to thank all the lecturers and staff of the University of Nairobi who took me through the entire course and availed the necessary material and information pertinent to my study.

Special thanks go to Mr. Henry K. Mwenemeru and Mr. Michael Mwangangi for their insights on concepts of the relatively new BYOD phenomenon.

Finally, I would like to thank all my family members and friends for their encouragement.

## Table of Contents

## List of Tables

## List of Figures

## List of Abbreviations

**BYOD** – Bring Your Own Device

**DVD R/W** – Digital Video Disk ReWritable

**ICT** – Information and Communications Technology

**IT** – Information Technology

**MAC** – Media Access Control

**MDM** – Mobile Device Management

**MICK** – Madison Insurance Company Limited

**NAC** – Network Access Control

**OS** – Operating System

**RAM** – Random Access Memory

**SD** – Secure Digital

**SSID** – Service Set Identifier

**VGA** – Video Graphics Array

# CHAPTER ONE

## 1.0 Introduction

### 1.1 Background

As defined by Cisco Systems Inc. (2012), Bring Your Own Device (BYOD) is "the practice of employees and business partners using their own devices to access data and run workplace applications." Cisco Systems Inc. (2012) also observes that today, the BYOD concept is having an impact on the way that we work and that some businesses are changing their entire IT strategy by providing employees with money to purchase devices of their choice rather than investing in a standardized desktops, laptops or Smartphones. According to (Alberta, 2006), the BYOD menu includes the following devices:

a. Laptop computers are portable computers that can be used with or without the Internet.
b. Netbook computers are portable computers that gain most of their functionality through the Internet.
c. Smartphones/handhelds, some of which blur the lines between the Internet and cellular networks for example Blackberry, Android, iPhone, personal digital assistants and the iPod Touch.
d. Tablet computers fall along a continuum from laptop-like to large size Smartphones such as iPad, Android tablet, et cetera.
e. E-book readers for example Kindle and Kobo.
f. Audio MP3 Players for example, the iPod.

As it is being witnessed, it is now a common acceptance for employees to acquire and upgrade their own BYODs as a means to facilitate both personal and business needs (Thielens, 2013). More so, the mobility advantage provided by these devices present great worth and thus fosters the BYOD embrace which has been fuelled by the advent of consumerization of these products. Enterprises across industries are starting to understand that they must adapt to 'consumerization of IT' (employees' introduction and adoption of consumer devices in the enterprise) and the remote working trends already underway in organizations (Thomson, 2012).

On the other hand, Antonopoulos (2011) observes that "the influx of BYODs has towed in tandem a myriad of interesting challenges for IT security administrators as these emerging devices introduce

new operating systems, new development environments and new information security vulnerabilities, threats and risks but in the contrary, no new controls.

### 1.1.1 Vulnerabilities, threats and risks

There exist numerous definitions of the terms “vulnerability”, “threat” and “risk”. In the words of Maniscalchi (2009), a vulnerability is “a flaw or weakness in system’s security procedures, design, implementation or internal controls which could be exploited (accidentally or intentionally) and result in a security breach or a violation of a system’s security policy.” On the other hand, a threat is “the potential for a person or thing to exercise, accidentally trigger or intentionally exploit a specific vulnerability; and risk refers to a situation involving exposure to danger (Maniscalchi, 2009)”.

## 1.2 Problem Statement

Anecdotal evidence shows that BYODs have made great headway into organizations in Kenya and that these devices have presented those charged with IT security with “food for thought” on how to appropriately embrace the new phenomenon gracefully. Madison Insurance Company Kenya Limited (MICK) is not unique to this trend. In a nutshell, at MICK, employees can be categorized in two namely high mobility employees such as marketers/sales agents, ICT staff and; low mobility employees such as insurance underwriters, accountants, actuaries, personal assistants and human resources staff. While high mobility staff is provided with laptops by the organization, low mobility staffs use desktop computers. However, both staff categories are allowed to use personal portable devices such as laptops, Tablets and Smartphones to access the organization’s ICT network and informational assets.

In order to access the network, these BYODs are delivered to the ICT department for configuration for wired connectivity. Alternatively, passwords to the wireless networks are provided to those who want to connect wirelessly. A challenge nevertheless arises because unlike with desktops computers, the ICT department has minimal visibility of these portable devices. As such, unmonitored numerous information security challenges emerge such as the possibility of data loss through device loss, classified files being copied on to the devices local storage, lack of adequate security measures on these devices (for example weak passwords), out of date antivirus programs, amongst others. To sum up, the ICT department at MICK is in the dark when it comes to knowing what was brought in vis-à-vis what has left the organization when it comes to these devices.

Suffice it to say that the introduction of the BYOD concept at MICK may have presented "Pandora's box" with regard to information security. As observed by Thomson (2012), the influx of consumer devices into the workplace requires more flexible and creative solutions from IT staff for maintaining security while enabling access to collaborative technologies.

The facilitator of MICKs BYOD information security challenge was the fact that a directive allowing the BYOD concept was incorporated as company policy (not ICT policy) before the ICT department established a BYOD adoption framework and policy that would have benchmarked its embrace. This directive's oversight therefore served as the impetus for this research which intended to investigate how user behavior had contributed to information security challenges at the organization and consequently led to the development of a BYOD adoption framework and policy recommendations for the organization because none existed. More so, it was evident that BYOD was showing new innovation paths for which there was a limited body of academic research (Disterer & Kleiner, 2013). This study served as a means of breaching this gap as well.

### 1.3 Research Outcome Significance

The BYOD framework and policy recommendation would define:

a. A suitable criterion for filtering devices which will be allowed to dock onto MICK's network.
b. BYOD user behavior benchmarks

### 1.4 Research Objectives

i. To review existing BYOD adoption frameworks that focus on curbing information security threats presented by BYODs.
ii. To identify information security threats the BYODs present at MICK.
iii. To poll BYOD user behavior to establish how this behavior facilitates information security threats.
iv. Probe the ICT department for infrastructure vulnerabilities presented by BYODs at MICK.
v. To establish whether BYODs threat to information security at MICK is real.
vi. To develop a BYOD framework and highlight policy recommendations that should be considered around issues identified in the BYOD adoption.

## 1.5 Research Questions

i. How does user BYOD behavior promote information insecurity?
ii. Do BYODs really present an information security risk at MICK?
iii. Can the threats presented by BYODs at MICK be identified and quantified?
iv. Will the creation and introduction of a BYOD framework and policy recommendations mitigate the perceived information security risk?
v. Will the developed framework and policy recommendations be unique to MICK or will it be applicable to other insurance firms?
vi. What are the deliverables of this research?

## 1.6 Research Limitations and Scope

The focus of this study was on all BYODs that dock onto MICK's network. The scope of this study was limited to MICK's BYOD users.

## 1.7 Justification

This dissertation had a scientific and psychological relevance. The scientific relevance was based on the fact that the BYOD phenomenon was a relatively new experience in most organizations in Kenya and thus literary material on the same was scant. As such, this study attempted to reduce that hiatus.

With reference to the psychological relevance, this study attempted to understand BYOD user behavior vis-à-vis information security challenges posed by of these behaviors. Conclusively, it was the researcher's intent to make a contribution towards building a workable BYOD framework and highlight policy elements which factor in technical and behavioral attributes that were necessary in ensuring a safe and secure adoption of BYOD phenomenon at MICK, and perhaps, other organizations as well.

# CHAPTER TWO

# 2.0 LITERATURE REVIEW

## 2.1 Introduction

The aim of this dissertation was to understand common user behavior that fuel information insecurity and the development of a suitable BYOD framework and policy recommendations that diminish security risks posed by the BYOD phenomenon to acceptable levels at MICK.

By looking at four existing BYOD models, it was the researcher's intention to single out core features presented by these models in the quest of identifying feasible features that were relevant in the development of MICKs BYOD framework and BYOD policy recommendations.

The research limited its scope to Madison Insurance Company Kenya Limited (MICK) for reasons that the company had embraced the BYOD concept. However, there existed neither a BYOD framework nor policy to govern the adoption of this phenomenon. As such, it was intended that at the end of the research, a BYOD adoption framework and a BYOD policy recommendation surrounding key identified areas of concern (with regard to user behavior) would be delivered in light of guiding the organization into securely adopting the BYOD concept.

## 2.2 Review of the Existing BYOD Arrangement at MICK

Anecdotal evidence gathered from MICKs ICT department heavily suggested that there was a looming disaster waiting to detonate by virtue of adopting the BYOD concept without having an adequate BYOD framework and BYOD policy in place. Employees were acquiring and presenting their devices to the ICT department for rudimentary configurations to allow them network access and thereafter they were able to access a myriad of network resources. It was worth noting that most of these devices (especially laptops) had been in use in other numerous networks and may have contained malware and/or software applications which provided "backdoors" that facilitated threats such as data leaks. Even so, most of these devices were not MICKs property and therefore, the ICT department could delete any data or uninstall any application(s) from these devices without the knowledge, consent and approval from their owners (of course, due to the lack of a BYOD policy catering for this).

## 2.3 Theoretical Review

In a much as BYODs bring the benefits of mobility, ease of use, increased computing power and combinations of interesting features, their adoption also brings in difficulties and risks. For IT security teams, the new risks typically includes security vulnerabilities (Romer, 2014). Attackers usually discover these loopholes and flaws in architectural design and exploit them to steal data, sabotage networks or even siphon funds (Romer, 2014). As stated by Johnson (2013), there is no panacea that would solve the numerous risks brought in by BYODs. "It requires not only carefully considered policies to be established and consistently applied across the organization, but also requires constant vigilance to keep those policies up to date with a fast-evolving ecosystem of devices, applications and user behavior" (Johnson, 2013).

The BYOD revolution has swept enterprises of all kinds. In organizations as diverse as law firms and manufacturers, employees are buying their own mobile devices such as Smartphones and Tablets and using them for work (Romer, 2014). Until the new technology matures, security teams find themselves racing to patch vulnerabilities, educate users, fine-tune processes, and deploy new security solutions tailor-made for the post-revolutionary world (Romer, 2014). As stated by Mwenemeru & Omwenga (2014), an unstructured technology adoption of BYOD concepts might be catastrophic to an organization in terms of security breaches, compromise in privacy and infrastructural control, amongst other vulnerabilities and threats.

As observed by Johnson (2013), legal issues must also be taken into consideration while adopting the BYOD concept such as who is to blame if unregistered software is detected in the organization. An oversight of this may propagate a quagmire of difficulties for an organization's ICT staff especially when coupled with the perpendicular technical and security challenges of managing a network that lacks satisfactory controls for the applications and devices that it connects.

It therefore emerges that employers require BYOD policies that address compliance and legal concerns, employee privacy, financial liability, appropriate device usage, Mobile Device Management (MDM) applications and local storage (Kulkarni et al., 2014). Additionally, according to Disterer & Kleiner (2013), there are compliance rules on company use which must be met such as requirements to document, archive, and back-up data. When mobile devices are designated for BYOD access for both private and business purposes ("dual use"), the end user's private data (contacts, addresses, photos, documents) must be protected against a company's access while access to company data is simultaneously guaranteed.

Another point worth noting is that never before have both privately owned and corporate data shared the same memory and storage space. This brings contention when matters concerning backing up of the data in mobile devices emerge because a clear separation of the two must be determined, with the isolation of business applications from the rest of the system being the goal. A lack of separation between private and business spheres yields significant risks for companies (Disterer & Kleiner 2013). A BYOD framework coupled by an adequate BYOD policy will most definitely bring into harmony how the adoption of the BYOD concept should be undertaken so as to prevent fears of susceptibilities to such foreseen eventualities.

Much not said, there also arises the technicality involved in the enforcement of BYOD framework and policies. According to Johnson (2013), there exists the ICT department challenge of carrying on its daily roles of network maintenance and effective delivery of reliable IT services while concurrently enforcing BYOD vigilance. Leaning too much on a policing role and ICT policy dictates will be portrayed as being cruel and oppressive vis-à-vis being respected.

In the words of Mwenemeru & Omwenga (2014), IT departments also have to grapple with the myriad of devices that penetrate through the doors of the organization every morning. Users usually have multiple devices which rarely match any preconceived notion of what a standard device should look like. Moreover, as asserted by Brandly (2011), IT departments drove technology in the past but the IT revolution has shifted the IT culture so that the users are the ones getting the latest cutting edge technology first and they want to bring these devices to work.

### 2.4 Benefits of BYOD

Over the years, the “Bring Your Own Device” concepts popularity has greatly swelled. As observed by Mwenemeru & Omwenga (2014), a survey by ISACA (2011) exposed that 54% of employees have a personal device that they use for work. The benefits accomplished by this is that company balance sheets now look healthier because of minimized hardware expenditure and users are happier because they work with devices of choice which they understand better and thus find them easier to use. In short, the BYOD concept is one that cannot be wished away by those organizations which are reluctant to adopt the paradigm.

Crook (2011) opines that, organizations that allow employees to work with devices that they are more comfortable with are inclined to have more satisfied employees and more so enjoy cost cutting (cited in Mwenemeru & Omwenga, 2014). Nihirika (2012) further states that such organizations benefit from

and retain top performers in the businesses, who seek to work flexibly, and, put in time outside of the traditional office hours for the benefit of the organization. The same is observed by Disterer & Kleiner (2013), who state that "the comfort offered by BYOD leads to a higher level of user satisfaction and productivity, which are also enforced by the following effects; users gain a sense of autonomy from the independent procurement of devices, users are more familiar with devices that they also use privately, and users do find consumer devices easier to use."

Overall, user satisfaction and productivity is considered to be a primary advantage of BYOD. According to a recent study by Forrester, 50% of 18 to 31 year olds and 40% of 32 to 45 year old workers believe the technologies they use in private life is "better" than those in their professional life. In the words of Morrow (2012), granting access to employees to the corporate network and thus information via unmanaged devices enables employees to work at any time, from anywhere, by using any endpoint.

### 2.5 User Behavior

Blythe (2013) reckons that organizations implement a variety of procedural and technical approaches to secure information such as data encryption and security awareness campaigns but these efforts are not enough as security breaches continue to plague companies. According to Blythe (2013), "statistics show that 93% of large organizations and 76% of small businesses experienced a security breach in the last year" and evidence seem to point to users as the source of the problem, due to failures to comply to the company's security policies either directly or otherwise. For instance, BYODs are typically used in various locations such as coffee shops, homes, hotels/restaurants and conference centers. The risk involved here is that an attacker would pry over the owner of a device with the intent of espying sensitive data or acquiring the devices password as it is being input. Even if the devices are used within the only organizations perimeters only, it is highly likely that the owner moves with the device from place to place within the organization thus making the device more susceptible to theft or loss (Keyes, 2014). This places mobile devices at a higher risk of compromise than the contemporary desktops.

A layered approach can be used to mitigate the risks involved high mobility. As stated by Keyes (2014), one layer involves protection of sensitive data by encrypting the devices storage so that sensitive data cannot be read by unauthorized parties or alternatively, not storing organizations sensitive data on mobile devices at all. The second layer involves requiring authentication whereby a user must supply a password (such as a domain password) instead of the user only using the devices

local password. Nonetheless, even though employees have been identified as the significant culprits to information security threats and vulnerabilities, information on this is fragmented and minimal effort to create theoretically based and empirically validated behavioral interventions has been realized (Blythe, 2013).

As cited in Allam et al., (2014), "information security awareness has been promoted as a means of reducing security risk across a number of threat areas." Kruger and Kearney (2006), Eminagaoglu et al. (2009), Albrechsten and Hovden (2010), and Bulgurcu et al. (2010) all promote awareness as a means of reducing security risk (cited in Allam et al., 2014). These authors explain that increasing awareness influences behavior, which ultimately reduces risk by focusing on the user and not the device. Unfortunately, as security risk areas are continuously changing and evolving, existing awareness quickly becomes obsolete, and therefore ineffective, with behavior having been found to slowly migrate back to higher risk patterns. This degenerative migration takes place without malicious intention. It has also been found that, as the operating environment changes and as risk changes, awareness levels are found to adjust accordingly."

It is thus of fundamental importance not only to have BYOD security policies and frameworks in place but to double this up with continuous user sensitizing on security awareness and, more so, on the importance of self security initiatives.

### 2.6 Risks of BYOD

The BYOD concept is a double-edged sword in that in as much as it bears great benefits to both the organization and users, "the convenience is accompanied by significant data security risks which can prove enormously costly" (Mwenemeru & Omwenga, 2014). This brings to the table the cardinal area of attention that BYOD information security should focus on. According to Keyes (2014), the most common BYOD data security concerns revolve around three major areas namely confidentiality, integrity and availability. Confidentiality ensures that the data/information being relayed cannot be read by unauthorized entities. Integrity on the other hand involves detection of any changes that are made on transmitted data (whether intentional or unintentional). Finally, availability refers to the guarantee that users can access resources through their BYOD whenever they require it.

Organizations which have not embraced the BOYD concept usually regard it to be a risky undertaking in two broad categories. The first relates to the fact that a company's data will be stored and transmitted using devices and networks which the employer does not own or manage. This loss of control may conflict with the increase over the last decade of government legislation requiring

companies to carefully protect the privacy and security of sensitive personal, financial, and health-related data; it can as well pose risks to the safety of a company's trade secret, proprietary, or confidential information.

The second set of risk relates to the impact of BYOD policies on the behavior of employees (Mwenemeru & Omwenga, 2014).

To add on, when people use mobile devices over wireless networks, there is usually a chance that the data being exchanged through the network can be accessed by an unauthorized third party (Mendez, 2012). This is where the use of Network Access Control (NAC) and Mobile Device Management (MDM) applications come into play. As explained by Mendez (2012.), Network Access Control systems, are used to monitor the company's network and perform checks on devices that try to connect to the organizations network. On the other hand, MDM is a system and method for remotely managing mobile devices (Danford &Batchu, 2013). Even more sophisticated than MDM is the concept known as containerization which involves creating an encrypted data store or container on a device that is accessible only with secure authentication, or credentials (Mendez, 2012).

According to research, mobile devices are already being used in around 80% of German companies for traditional telephone communication, for functions of a traditional telephone system (including short cuts, forwarding calls), for e-mail, and for access to centralized calendars and contact information. In the USA and Europe, 60% of companies have set up BYOD programs for Smartphones, and 47% have done so for Notebooks and Tablets. However, these figures do not reveal the extent to which utilization goes beyond rather simple telephone communication and e-mail. The fuzzy figures on prevalence reveal the need for differentiation. Distinctions should be made based on ownership of device and on using devices for telephone and e-mail or beyond (Disterer & Kleiner, 2013).

As stated by Allam et al. (2014), despite Smartphones being property of users, they are increasing being used to access corporate networks and process organizational information perpendicularly with personal information, though users are seldom aware of the threat that these devices bring in or, even if they have some level of awareness, how to diminish these risks. The situation is worsened by the reality that Smartphone owners are exclusively responsible for the ultimate administration of their own devices (Allam et al., 2014).

Research by the Ponemon Institute (2012) confirms that in the past three years mobile devices have become a major threat for 73% of their respondents, up from only 9% in 2010. A study by Cisco

(2013) found that almost 40% of Smartphone users do not have a password enabled on their device. A similar study by PricewaterhouseCoopers (2012) estimated that as many as one in three small businesses, and 75% of large businesses, allow Smartphones and Tablets to connect to their systems, many without taking any steps to mitigate potential risk (cited in Allam et al., 2014). The vital point here is that information which historically used to be protected behind firewalls, secured servers amongst other security measures, is now finding its way into inadequately protected personal mobile devices (Allam et al., 2014).

Currently, statistics show that mobile devices are clear leaders in the list of the most significant security threats, as confirmed by security experts' study involving companies from various industries (Disterer & Kleiner, 2013). The rudimentary virtues of authenticity, confidentiality and integrity are those that are faced with the greatest threat. With regard to confidentiality, the peril arises when unauthorized parties obtain access to material that is classified. This is achieved through either intercepting data transmissions or manipulating devices. Manipulation is usually performed by utilizing inadequately secured devices which in effect threatens the confidentiality of corporate data (Disterer & Kleiner, 2013).

On the other hand, authenticity is jeopardized when devices are used to elicit business dealings that are difficult to trace clearly and without doubt. Disterer & Kleiner (2013), assert that insufficiently secured mobile devices are in the lead when it comes to unauthorized use and alteration of data due to deliberate or negligent actions. It can be implicitly assumed that the negligent or incautious behavior of users during private use will be transferred to business use.

As noted by Morrow (2012), according to the 'Internet Security Threat Report' in 2011 by Symantec, more than fifty (50%) percent of mobile devices currently contain threats that gather user data and track user activities. More so, about a quarter of identified mobile threats were discovered to be collecting and sending user personal information. As such, it is worth noting that the latest trend of malware is that they are being written for purposes of information collection. Morrow (2012) also notes that users are installing a wide range of applications on their mobile devices that can potentially be malicious and put data at risk. A sloppy employee who accesses the corporate network through an unmanaged device can unintentionally leak information merely by saving a file opened from Webmail or SharePoint to their mobile phone file system. This can then be easily stolen by a malware application designed to access the SD card on the mobile device. Lately, Morrow (2012) adds that mobile device malware are being written especially for the Android operating system. This is a rising threat, albeit also for OS-modified (also known as jail broken) iPhones. Suffice it to say that just as the

Windows' larger market share draws a bigger number of threats vis-à-vis Apple or Linux, Android's rising market share is equally attracting an increasing number of mobile malware threats.

To add on, it can be anticipated that ICT departments will have to support a larger number and broad spectrum of devices with these devices being changed every so often as is often the norm of users, especially, those who cherish possession of the latest releases of devices as opposed to company owned devices which are changed less regularly.

Nonetheless, as observed by Disterer & Klein (2013), there arises the need for assistance by users in installing software and the registration of privately owned devices. In the event of device loss and technical challenges, users expect ICT department services. Without ICT policy, questions such "which measures are predetermined if a device is lost as a result of misplacement or theft?", "how will data stored locally on the personal device be wiped out?" and "will the employer provide replacement devices so that users can continue to work?" become very difficult to answer.

In today's on-line world, employees are also demanding for flexible working hours and employing the advantages of mobility provided by mobile connectivity in order to boost productivity. In a recent employee survey by Forrester, 42% of respondents admitted that when it comes to getting their work done, they will use a personal computer or Smartphone; a strong indication that the BYOD trend is indisputably here to stay (Khanna, 2013). This presents a challenge to businesses as to whether to endorse a BYOD policy and more so, about admitting that it is already taking place and enforcing data security policies that are flexible enough to protect organizational information assets regardless of the endpoint devices (Khanna, 2013).

As also asserted by Khanna (2013), there exists numerous drawbacks of employees accessing sensitive corporate data from unmanaged devices and that for such an environment, it is more plausible to secure the data as opposed to securing the end devices. This means looking at security from the data's perspective for example through encryption; and from the perspective of data loss, that is, during data transfer. Nonetheless, the solution must be flexible enough to offer usability and system integration so as to foster data security throughout the business at all times.

In the words of Khanna (2013), while 91% of businesses consider data security to be their number one IT priority, 21% of businesses do not have a policy to safeguard against data sharing across consumer-grade platforms; a contradiction because figures reveal that many data breaches as resultant of internal laxity over data control (Khanna, 2013).

In determination to do their job coupled by work pressures and ever challenging occupation challenges, today's worker will employ any available solution, be it Dropbox or Google Drive. With numerous of these solutions, IT do have a challenge when it comes to protecting data against this influx of applications, in that, these solutions bear terms and conditions for use that may grant the provider with rights to read, replicate or even redistribute data stored therein all in the name of trying to offer the user with better services (Khanna, 2013).

Suffice it to say, as stated by Khanna (2013), "in a climate of 'bring-your-own-everything', it is the IT department that has the power to put in place solutions that are effective despite the fluid use of devices and technologies: Security today is about flexibility not rigidity".

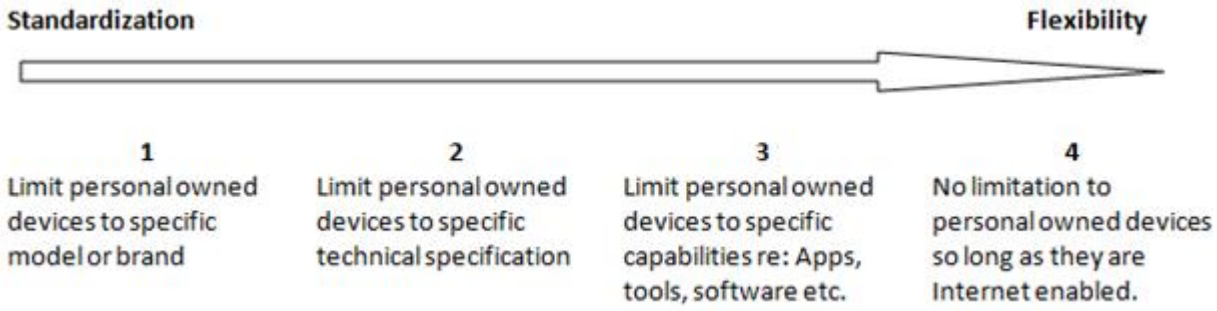
## 2.7 Existing BYOD adoption Frameworks

According to Alberta Education (2012), the model of BYOD framework for adoption is influenced by the level of needs. More so, the decision as to which BYOD model is adopted has major implications for users, IT administrators and the organizations policy makers. Nevertheless, the policies that are instituted about which devices are acceptable as personally owned devices, in turn, impact what the users and IT administrators can do with these devices at the workplace (Alberta Education, 2006).

### *2.7.1 Integrated Framework of BYOD adoption*

In this framework, a variety of acceptable devices fall into a continuum that range from high standardization to high flexibility as depicted in Figure A below. One side of the range (standardization) is the identification of a single type of device that users must acquire whereas the other extreme (high flexibility) represents an open-ended framework that allows users to bring in any device of their choice (Mwenemeru & Omwenga, 2014). As stated by Alberta Education (2006), the limitations of the integrated model include limiting devices to a specific model or brand, limiting devices according to definite functionality, limiting devices to specific technical specification and that are internet ready.

**Figure A: Integrated Framework Model**




*Source: Alberta Education (2012)*

### *2.7.1.1 Limit personally owned devices to a specific brand/model of device*

This model limits user devices to specific brand/model of devices. For example, "Users will be expected to purchase HP Pavilion 15 laptops for their office work whereas all other devices will not be allowed into the organization".

As opined by Alberta (2006), this model has its advantages such enabling the ICT department know device capabilities, plan on which applications that are compatible with these devices, facilitate ease of configuration of devices due to the absence of a learning curve, ease of technical trouble shooting and the standardization of device charging stations. However, the detriments of this model include inflexibility related to choice and device preferences and thus difficulty in enforcing this model as policy (Alberta, 2006).

### *2.7.1.2 Limit Personally Owned devices to a meet specific technical Specifications*

Although this model may permit any devices brand/model, it limits user devices in terms of technical specifications such as specific types and versions of Operating Systems, allowable minimum amount of storage space and Internet readiness, to mention a few. An example of this would be "Users are required to purchase a laptop that runs Windows 8.1, has a VGA (Video Graphics Array) card and has a DVD R/W Drive" or "Users will be required to purchase laptops with Core i5 processors, 500GB Hard Drive and 4GB RAM (Random Access Memory)". The advantages with this model are that there is flexibility in device choice and IT departments are aware of the applications that can run on devices. In contrast, the disadvantages include challenges in IT department's technical support due to various platforms, IT have to confirm whether applications run on different platforms such as Linux and

Windows before acquisition, lack of standardization limits possibility of standardizing charging stations and challenges in updating the brand/model (Alberta, 2006).

#### *2.7.1.3 Limit Personally Owned Devices to Specific Functionality*

This model involves limiting BYODs to specific functionality such as compatibility with software or compatibility with on-line testing requirements (Alberta, 2006). For example, "Users are encouraged to bring personally owned devices that can connect and interact with the core Insurance System, allows creation of full text documents and that can run on-line interactive software or simulations based on the Flash platform" (Alberta, 2006). The main advantages of this model are that users have some flexibility with device choice. However, user may be unsure on how to identify a device that meets this requirement and/or may be forced by circumstances to buy new devices. This makes it difficult in enforcing this as policy (Alberta, 2006).

#### *2.7.1.4 Accepting All Personally Owned Devices Provided They Are Internet Ready*

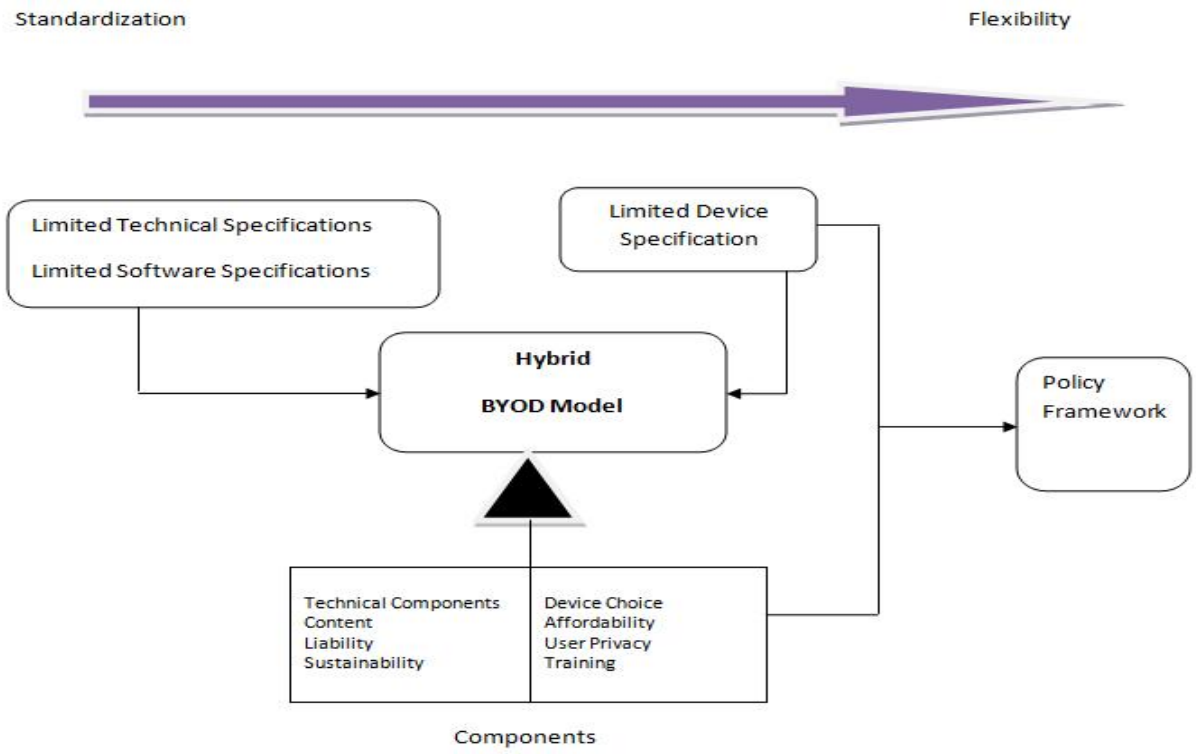
This model offers the highest flexibility in that users can bring in any device the only condition being that the device must be capable of connecting to the Internet. For example, "Users are allowed to bring personally owned devices to work on conditions that the device can connect to the Internet and therefore also the school network" (Alberta, 2006). The advantages of this model are that the users have great flexibility in device choice, the IT department leaves the headache of technical challenges to the users and users rend to understand the pros or cons of their devices. However, the downfall is that users may become incapable of utilizing their devices due to pedagogical requirements (Alberta, 2006) consequently affecting their capability to work with their devices.

### *2.7.3 Hybrid Framework of BYOD Adoption*

The hybrid framework borrows its features from combinations of the four categories listed above. An example of adoption could be "Users can use any device with wireless capability is permitted to connect to the organizations network provided the user has a login account and agrees to behave as stipulated on the ICT policy" (Alberta, 2006). The advantages and disadvantages of the Hybrid Model vary according to the combination (hybrid) chosen.

The attractiveness of these models is the flexibility and the fact that it takes into consideration the underlying organizations infrastructure (Mwenemeru & Omwenga, 2014). The figure below depicts the hybrid model.

**Figure B: The Hybrid Model**




*Source: Mwenemweru & Omwenga (2014)*

When it comes to BYOD, there is a no one-size-fits all model. As clearly seen, although all these models are excellent models, they are device-centric meaning they address devices allowable on the network sufficiently with concerns only on the constructs of hardware and software. They however do not shed light on constructs of policy matters and/or how they can be incorporated adequately. Yet, a key question is how to handle BYOD related cases when such matters arise especially issues relating to user behavior such as awareness and trends so as to curb behavior that may be foster information insecurity. It is therefore important to also evaluate pertinent policy models that will guide MICK towards handling matters BYOD.

## 2.8 BOYD and Policy

As stipulated by Armando et al., (2012), organizations must have security policies that participants must accept and respect. Such policies are to be devoted to a two-fold aim, namely avoiding users introducing malicious software inside the organization (outsider threats) and secondly, ensure users do not take outside sensitive information from the organization (insider threats).

According to Bradford Networks (2014), as companies' are in transition to BYOD environments, the following questions come up time and again:

a. How do you know what devices are connected to your network, and if they are authorized?
b. How do you know if employee-owned devices are up to date with the latest operating system versions and anti-virus/spyware software? How can you enforce this?
c. How do you let employee-owned devices safely onto your network?
d. Will they be full-function or restricted to specific apps, locations etc?
e. How do you enable but limit network access for contractors, partners, project teams and other guests?
f. When responding to an incident, can you replay the Who/What/Where/When of network access?

These questions need to be addressed with criticality in order to have a successful BYOD adoption. To add on, as we are headed to a world of foreign devices with complex features, BYODs are increasingly demanding a new method of network access control. A new generation of Network Access Controls (NAC) is therefore required by organizations to manage these emerging complexities (Bradford Networks, 2012).

### *2.8.1 Ten Steps to Secure BYOD*

Bradford Networks (2012) prescribes ten steps to ensure a secure BYOD environment that works for both users and the organization. This approach focuses on a flexible policy-based network provisioning that that can also support mobile devices and thus shifts its focus from the traditional command-and-control and ensures employees can work on their devices without jeopardizing organizational information security. The ten steps outlined by Bradford Networks are:

a. **Determine which mobile devices are allowed on the network**

   This involves determining what devices need to be supported and if those devices are secure enough to be granted network access. A company may allow any device guest access and specific devices, further access. It is also important to educate employees about security practices at this stage and if a device cannot be supported because it is highly insecure, this is

the stage where it is explained why. The IT department should also reach out to different departments to understand the BYOD needs rather than attempt to make decisions on its own.

**b. Determine which OS versions are allowed on the network**

At this stage, there is need to determine which type of OS (operating system) version that need to be installed on each device and that make sure that software patches are up-to-date to abate susceptibility to viruses and spyware. Mobile Device Management (MDM) software that users download can ensure this and more so enable device wipe if the device is reported stolen or lost.

**c. Determine which applications are mandatory/prohibited for each device**

Here, applications that are mandatory to enable employees to be productive are determined. ICT administrators can use MDM software to configure network access only to specific enterprise applications and prohibit access to personal applications that could present a security risk. When the user logs out of the company network, they can go back to using their personal applications. However, a lenient policy may also allow users to log on to their applications as long as they are from a trusted source, such as an app store. The MDM software can also tell if the device has been tampered with (jail-broken) and downloaded software that is potentially not from an app store thus less secure. As such, depending on policy, this device can be disabled or the user given limited or guest status.

**d. Determine which groups of employees will be allowed to use these devices**

This stage involves determining user profiles in terms of what privileges they have, what device they are using and what applications they need to use. For example, a sales officer may be granted access to view the sales he/she has made whereas the head of sales can have access to viewing all the sales made by the entire sales team. There exist Network Access Control technologies to facilitate this.

**e. Define who, what, where and when of network access**

In this step, users and groups are associated with a specific network according to policies defined. For example, if the head of ICT wants to access MICKs Mobile Money records from his iPad, a unique identifier such as the iPad's Media Access Control (MAC) address to identify his device, identify the owner, specify a Service Set Identifier (SSID) that identifies the wireless network and specify the physical Access Point(s) from which that network can be accessed. This can also be facilitated by the Network Access Control application. These "Who/What/Where/When" specification that define access for the head of ICT can now be carried over, with suitable modification, to other parts of the organizations premises.

**f. Educate employees about the BYOD policy**

By reaching this stage, the BYOD policy is ready and it is important that users understand it as well as the reasoning behind it. They also need to understand that the policy will be enforced. It is important to note that effective communication essential for a successful BYOD program. Most security issues that arise in organizations are caused by users who are unaware of the rules. Since employees are going to buy personal devices, it is important to be sure they know what to get.

**g. Inventory authorized and unauthorized devices**

Since a network access policy cannot be created and implemented in a vacuum, before setting up controls, there is need to conduct a check to see what devices are currently on the network and who is using them. This makes sure that that the access policy defined is sound and in line with employee requirements and preferences. The information gathered here can then be used to stream the BYOD policy if necessary before starting to enforce it in Step I.

**h. Inventory authorized and unauthorized users**

It is vital to keep track of known and unknown users who are currently accessing the organizations network ad what devices they are using. Steps 7 and 8 give a complete view of the BYOD environment: What devices are accessing the network, Who owns them, What company applications they are accessing and What personal applications are running in devices (including applications with vulnerabilities that could put the organization at risk).

**i. Control access based on the need to know**

After building the network access policy, educated the users about the BYOD initiative, used network visibility to inventory devices and users currently on the network, this stage entails enforcing the network access control policy, that is, the Who, What, Where and When of network access control. This stage is automated since there are technologies that handle this. Any unidentified user who attempts to access the network is either rejected or granted minimal privileges such as Internet access for checking email while being denied access to back end servers,

**j. Continuous vulnerability assessment and remediation**

This stage involves continuously checking for vulnerabilities and the organizations changing needs and modifying the policy to reflect these needs as well as evolving security threats.

## 2.9 The Optimized Hybrid BYOD Framework

The aforementioned BYOD adoption frameworks are all admirable but are however heavily focused on an organization's vetting allowable devices as opposed to policy reasons being that organizations policies are internally driven to suit specific needs. Ultimately, the success of your BYOD program is measured by employees' willingness to use their personal devices within the rules set for them. An organization's security procedures and policies should determine the 'whether and how' of BYOD adoption (Eschelbeck and Schwartzberg, 2012).

With reference to devices, they are categorized in terms of limiting them to specific brand/model, specific technical specifications, specific functionalities and allowing all devices. A common deficiency in these models is that network access policies are not defined. As such, the incorporation of Bradford Network's "10 Steps to Secure BYOD" into the one of the BYOD adoption frameworks (or a hybrid), should help and organization achieve its secure BYOD paradigm adoption. This can be achieved by merging a suitable model (or hybrid of models) and consequently applying Bradford Network's10 Steps to secure BYOD and in effect create the self-contained "MICK – Hybrid BYOD adoption framework". This framework will be an apt BYOD solution as it will address both the devices and network access control with the aim of achieving a secure formal BYOD program. As quoted by Eschelbeck & Schwartzberg (2012), "You need to formalize policies specifically around BYOD".

### 2.9.1: The Optimized Hybrid BYOD Conceptual Framework

#### a. BYOD Flexibility Model

The MICK-Hybrid BYOD model adapts the BYOD Flexibility Model's feature from the Integrated Framework. The rationale behind the choice of the flexibility model is that it permits users to bring in any device the only condition being that the device must be capable of connecting to the Internet. This feature is ideal for MICK in that the organization has already allowed staff members to use BYODs without having thresholds to define the types of allowable BYODs in the organization. To add on, any attempt to filter the BYODs presently is bound to face steep resistance from staff considering the fact that users have already spent money to acquire these devices.

**b. Network Access Controller (NAC) and Mobile Device Manager (MDM)**

As earlier explained, Network Access Control (NAC) systems will monitor the company's network and perform checks on devices that connect to MICK's network and request utilization of network resources. These NACs checks will restrict availability of network resources such as applications, storage, emails, organization calendars, Internet access to certain sites etc to BYOD that will comply with MICK's define BYOD policy. As asserted by Pham et al. (2005), the NAC system operates as a secure portal for network resource operations between BYODs and network resources. This system (either appliance/software) either allows or terminates network resource access transactions identified on the basis of packet information which includes clients' system and mount points supported by the access controller (Pham et al., 2005). Based on packet information, the policy parser within the NAC) selectively determines initiations of network access transactions between the NAC and network resources (usually hosted in the data center) to enable completion of transactions directed from the clients towards the NAC (Pham et al., 2005). It is important to note that the policy parser is informed by the organizations ICT network access policies.

The Mobile Device Manager (MDM) which will deal with the administrative task of deploying, securing, monitoring and management of BYODs so as to optimize security and functionality of these portable devices at MICK. As stated by Stricklen et al. (2008), the MDM utilizes an enterprise's existing organizational structure to define management permissions for BYOD administrators and users in addition to defining policy configurations and schemes for BYODs.

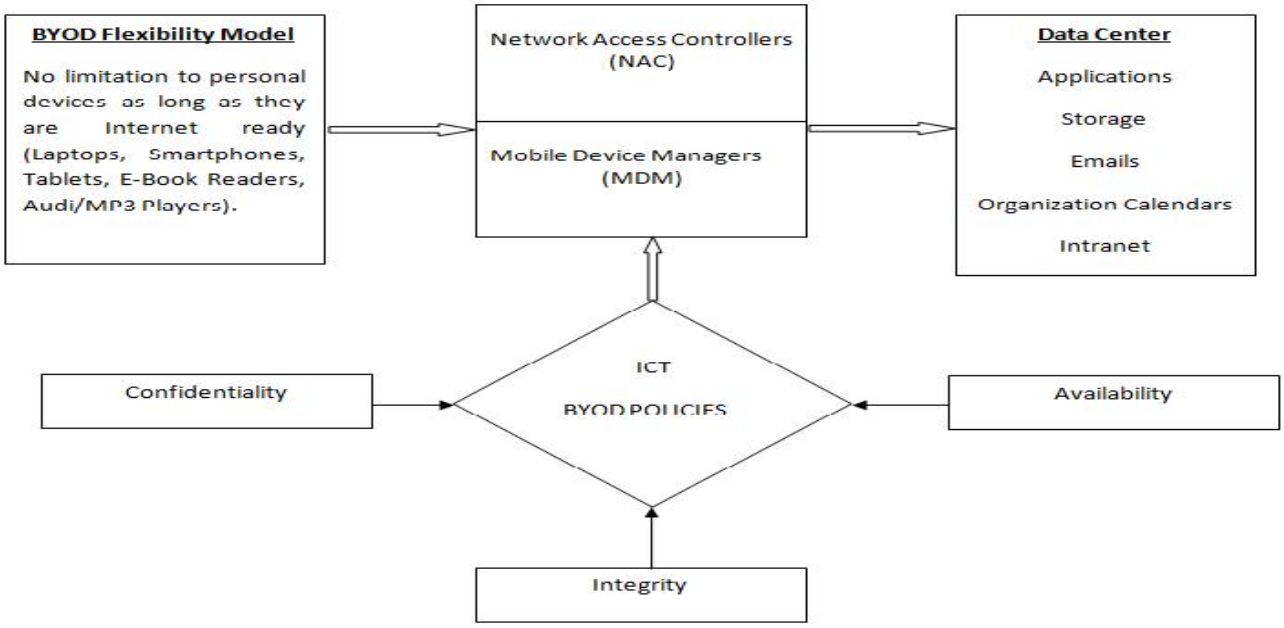
**c. ICT BYOD Policies (Embracing Confidentiality, Integrity and Availability of network resources)**

The MICK ICT policy is the receptacle that holds rules which shall govern BYODs at MICK. This receptacle will host rules derived from data confidentiality, data integrity and data availability domains around which information security revolves (Keyes, 2014).

**d. Data Center**

The data center is the core "container" of all network resources at MICK. It hosts applications such as the core insurance systems, the human resource systems, finance systems, routers, firewalls, IPBX, core switches etc. This is the ultimate resource point which all BYODs intend to access. In order for BYODs to securely access data center resources, they will have to undergo vetting from the NAC and MDM which will contain access control policies derived from the BYOD ICT policies.

**Figure C: The Optimized Hybrid BYOD Conceptual Framework**



# CHAPTER THREE

# 3.0 METHODOLOGY

## 3.1 Introduction

This chapter takes a deeper look at the steps, procedures and methodologies that were used for data collection, measurement and data analysis that were in line with the acknowledged objectives.

## 3.2 Research Hypothesis

This research hypothesized that risky BYOD user behavior inferably promoted information insecurity within the organization which was attributed to the lack of a BYOD policy at MICK. This was to say that the lack of a BYOD adoption policy for MICK employees had encouraged certain dangerous BYOD user behaviors to thrive. The behavioral outcomes were addressed through two perspectives namely (i) Assessment the levels of user awareness on matters relating to BYODs; and (ii) BYOD user behavioral attributes which encouraged information insecurity. As such, this research supposed the following:

**(i) Inadequacy of BYOD user awareness**

The existing user awareness gap included but was not limited to:

a. Knowledge on the aspects of information security.
b. Understanding of what malware was and the dangers they pose.
c. Knowledge of what software updates/patches were and installation of the same.
d. Implications or consequences of using mobile devices on public networks.

**(ii) BYOD user behavioral attributes**

The lack of a BYOD adoption policy had effectively enabled MICK agents to exercise certain risky behavior (either knowingly or unknowingly) with regard to information security. These included:

a. Use of BYODs on other networks (wired or wireless) such as coffee shops, restaurants, other offices.
b. Usage of antivirus programs which were not up-to-date.
c. Storage of company data such as email correspondences and file attachments on personal devices.
d. Security measures/methods MICK staff had on their devices

e. Strength of security measures MICK staff had on their devices such as password, pattern codes, PIN codes and biometrics.
f. Sharing of security measures/methods with other people.
g. In general, the frequency the security measures/methods were changed.
h. Request of other IT savvy friends/people to troubleshoot user devices other than MICK's ICT staff.

On the other hand, in order for BYOD user behavior to be considered as risky, certain vulnerabilities must have existed on MICKs ICT infrastructure. This research therefore also aimed at identifying known information security threats that these devices were posing on the organization as viewed by the ICT department by addressing the following three areas:

**(i) Identification of information security threats the BYODs present**

Since MICK ICT was devoid of a BYOD policy, this research supposed that:

a. No threshold existed that allowed/prohibited devices that dock on MICKs network
b. ICT had no visibility of MICK employee's devices that accessed company information.
c. That numerous threats existed.
d. That known existing threats had not been documented.
e. That certain steps had been taken to mitigate known existing threats.
f. That it was not mandatory for BYOD users to change their passwords.
g. That BYOD users were not educated on the importance of running updates, importance of data encryption, the need to urgently report data security issues and the importance of changing device PINs and passwords regularly.
h. That certain concerns arose when BYOD users accessed work related information or applications such as employees abusing BYOD, security of the devices, data protection, visibility of all devices that were accessing the organizations informational assets, compatibility of the devices, performance of the device and provision of IT support for personal devices.
i. That the organization believed BYOD benefits outweighed the risks.

**(ii) Audit the vulnerabilities of MICKs IT infrastructure**

This research proposed that:

a. That MICK did not have a means (such as a Mobile Device Management application) of monitoring BYOD activities.
b. That MICK had no vetting criteria (either software, hardware or both) of mobile devices that were allowed to dock on its network.
c. MICK had not explicitly stated which group of users was allowed to use BYODs.
d. That no criteria of who, what, where and when of network access had been established.
e. That authorized/unauthorized devices were not inventoried.
f. That no actions were taken on a new user's device when they joined MICK.
g. That no actions were taken on a user's device when they left MICK.

**(iii) To develop BYOD adoption policy recommendations around the issues identified**

At MICK, no BYOD adoption policy existed. In order to mitigate information security risks that these devices presented, a BYOD adoption policy needed to be developed and put in place. It was this research's intent to give BYOD policy recommendations as its deliverable. This was driven by the following hypotheses:

a. That MICK did not have a formal BYOD policy.
b. That the BYOD was to cover fundamental BYOD information security issues.
c. That the BYOD policy was to address all the fundamental concerns as outlined by MICKs ICT department.

It was the goal of this research to determine the likelihood that information security at MICK was rife because the lack of policy promoted reckless behavior or in the contrary determine that the absence of a BYOD policy had no influence on risky user behavior.

## 3.3 Research Design

As defined by Kothari (2008), "research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy procedure therefore giving structure in which the research is conducted and, it contains the collection, measurement and analysis of data".

This research employed survey research design. On one hand the researcher, using simple random sampling, sampled a group comprising of MICK's employees for inclusion in the study. The employees' BYOD user behaviors were assessed with the aim of establishing how these behaviors promoted information security threats, and, on the other hand an audit of MICKs infrastructure for BYOD vulnerabilities was conducted in order to establish whether BYOD threats to information security at the organization were real. The researcher also used an expert sample comprising of members of the ICT department in order to (i) Identify information security threats the BYODs were presenting (ii) Audited the vulnerabilities of MICK infrastructure with regard to BYOD and finally (iii) Developed a secure BYOD framework by identifying and exploring key areas of concern that need to be given attention to in order to guarantee a seamless, safe and secure BYOD program adoption at MICK.

Thomson (2012) observes that the influx of consumer devices into the workplace will require more flexible and creative solutions from IT staff for maintaining security while enabling access to collaborative technologies. At MICK, employees took their personal devices (as stipulated in the corporate policy) to the ICT department for network configuration. Thereafter, these devices gained access to the organizations network resources upon basic authentication (just as desktops). However, unlike desktop, the ICT had minimal visibility of these devices. This brought about numerous security challenges, known and unknown, such as possibility of data loss through device loss, classified files being copied on to the devices local storage, lack of adequate security measures on these devices for example weak passwords, out of date antivirus programs, amongst others.

Instead of denying people use of these devices for fear of information security risks, organizations ought to adopt the 'bring your own device' vision and by doing so, focus on business solutions through enabling technologies that meet this challenge.

### 3.4 Target Population

The target population for this research was divided into two categories.

i. ICT Staff – This group comprised of Head of ICT, IT managers, Systems Analysts, Systems Administrators and Networks Administrators. The intent of having this group was to get expert opinion's take on the following objective:

a. Establishment of whether BYODs threat to information security at MICK was real and the threats it posed.

ii. Employees of MICK – This group involved MICK members of staff (users) with the intent of understanding user behavior so as to satisfy the following objective:

a. Polling BYOD user behavior to identify commonly known information security threats BYODs that were present at MICK.

## 3.5 Sampling

Due to the fact that it was too costly to sample the entire MICK corporate family, random sampling for qualitative analysis and expert sampling for quantitative analysis was employed.

### *3.5.1 Random Sample*

MICK's employees were spread across 21 branches nationwide. These employees are subdivided into groups known as Units. Every MICK branch approximately had four (4) units, making a total of eighty four (84) units. The researcher randomly singled out four (4) employees per a branch to create a total of eighty four (84) respondents who gave their feedback through questionnaires. The rationale behind this choice was to have representation from each and every MICK branch in addition to giving every employee an equal possibility of being selected. This sampling frame was representative of the entire population.

### *3.5.2 Expert Sample*

This constituted of more specific respondents and the research instrument used was also a questionnaire. The respondents had to be specific because the survey inquiry required those with specialized knowledge to give their opinions. As such, the sample identified for this purpose comprised entirely of the ICT department staff and especially those who were in domains of authority. This sample group included the Head of ICT, two (2) ICT deputy managers, one (1) Systems Analyst, one (1) Systems Administrator and one (1) Network Administrator making a total of six (6) respondents.

## 3.6 Research Instruments

To accomplish the data collection required for this research, the research instruments used were questionnaires. These instruments provided a good source for accurate information with regard to the scenario on the ground. They were also relevant sources of information for identifying pertinent issues that were to be considered by the organization in the development of a BYOD policy.

### *3.6.1 Questionnaires*

Questionnaires were used as the method of collecting user data because they were inexpensive and had the ability to eliminate prejudice. Both closed and open-ended questions were be utilized as this research was both qualitative and quantitative. The questionnaire was be based on the constructs of the issues that were to be investigated.

### *3.6.2 Observation*

Due to the information security aspect of what was to be observed, there was immense likelihood of stage-managed behavior. As such, gathering data through observation may have yielded prejudiced results and therefore inaccurate analysis. However, an attempt on user behavior observation was made especially with focus on measures users undertook such as locking devices when on coffee breaks and how securely users supplied passwords when prompted to do so by their devices but this was not successful.

### *3.6.3 Secondary Research Methods*

In order to achieve in-depth understanding of the problem domain, several literary works related to the BYOD were reviewed so as to shed more light in the realm of BYOD security and adoption. Other BYOD frameworks namely the integrated framework, Specific functionality framework, the Hybrid framework and the Bradford Network's "10 Ways To Secure BYOD" were also reviewed.

### *3.6.4 Testing Research Instruments*

In the words of Mugenda & Mugenda (2013), "the results of a research depends on a large extend on the accuracy of the data collection procedures". In order to increase the validity and reliability of the research instruments, it is crucial to test the utilized test instruments. The questionnaires were tested by

being subjected to fifteen randomly selected MICK employees who checked for vagueness and ensured ambiguity was eliminated. Thereafter, the unclear statements were amended to establish clarity. The same process was applied on the expert questionnaire where five (5) randomly selected ICT support officers tested it for vagueness and clarity of the questions after which ambiguity was eliminated.

## 3.7 Data Analysis

In order for raw data to make sense, it must be processed and analyzed. Therefore, the data was subjected to editing of errors identified, identification of omissions and correcting them, data classification for purposes of identifying relationships and finally organizing of the data in such a way that aided analysis. This simplified the qualitative and quantitative data analysis methods.

### *3.7.1 Quantitative analysis*

For closed-ended questions, in order to arrive at information that assisted in describing distribution of scores, the quantitative approach was used. This strategy was used because the population sample was homogenous. This was executed through collecting numerical data that was analyzed using the Statistical Package for Social Sciences (SPSS). Both descriptive and inferential statistical data analysis techniques were applied. According to Creswell (1998), descriptive data analysis involves organizing the data into a frequency distribution, graphs, describing what the data average is or the typical distribution of a data set, describing the variability within a distribution while inferential statistics provides an in-depth analysis to draw deductions into the relationship between a set or two or more variables.

### *3.7.2 Qualitative analysis*

For open-ended questions, the qualitative approach was applied to analyze the data collected so as to arrive at meaningful deductions which aided in the identification of trends. This was done through probing on different ICT department's perspectives, experiences, challenges and position around MICK's BYOD needs vis-à-vis information security.

### 3.8 Mapping the Research Objectives on to Methodology

| No. | Objective | How Objective was achieved |
|---|---|---|
| 1 | Review of existing BYOD adoption frameworks that focus on curbing information security threats presented by BYODs. | BYOD frameworks namely the integrated framework, Specific functionality framework, the Hybrid framework and the Bradford Network's "10 Ways To Secure BYOD" were reviewed. |
| 2 | To identify information security threats the BYODs present at MICK. | Probed the Head of ICT, ICT managers, Systems Analyst, Systems and Network Administrator on their opinions on BYOD and security. |
| 3 | To poll BYOD user behavior and identify commonly known Information Security threats BYODs present at MICK. | Used questionnaires designed in a manner that elicited responses on how users behaved under different circumstances. |
| 4 | Audit the vulnerabilities of MICK infrastructure with regard to BYODs. | Probed the Head of ICT, ICT managers, Systems Analyst, Systems and Network Administrator on MICKs perceived network vulnerabilities posed by BYODs. |
| 5 | To establish whether BYODs threat to information security at MICK is real. | Analyzed data collected for cause and effect between user behavior and information security in order to determine the assumed hypothesis. |
| 6 | To develop a BYOD secure framework around issues identified as appertain BYOD adoption at MICK. | After data analysis, developed a BYOD framework policy recommendations for MICK that was in-line with and fostered a secure BYOD adoption which factored-in user behavior considerations. |

# CHAPTER FOUR

## 4.0 FINDINGS AND DISCUSSION

### ANALYSIS RESULTS

As earlier discussed MICK employees are spread across twenty one (21) branches nationwide and the same comprised the sample group. Each branch has four (4) units, making a total of eighty four (84) units. The researcher randomly selected four (4) employees per branch representing an employee from each of the four (4) units in each branch. The employee poll was conducted in a manner aimed at establishing two aspects namely user awareness and user behavioral trends with reference to so as to establish how these two aspects promote information insecurity.

The data extracted from the research instruments (questionnaires) was analyzed using Statistical Package for Social Sciences (SPSS) Version 22.

The demographic characteristics of the eighty four (84) respondents, MICK employees, were graphed and displayed as shown in the figures below:

### 4.1 Respondents' Characteristics

***a) Age Distribution***

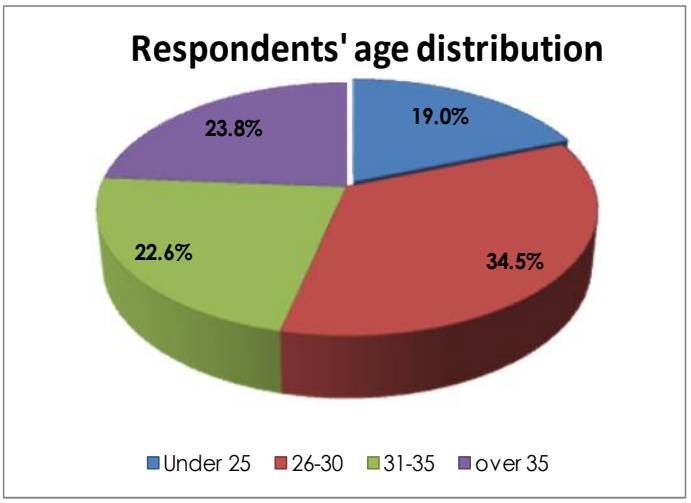



***Figure 4: Age distribution***

As displayed in pie chart Figure 1 above, a majority (34.5%) of the respondents (MICK staff) fell within the 26 – 30 years age bracket.

***b) Academic Qualification***

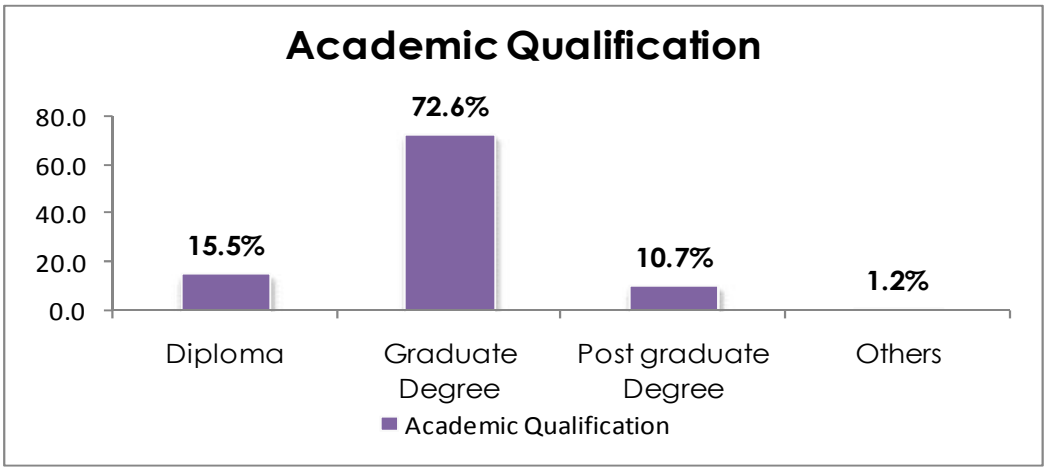



***Figure 5 Academic qualification***

As graphically displayed in Figure 2 above, majority (72.6%) had a graduate degree academic qualification.

## 4.2 User Awareness

### *4.2.1 Devices that respondents own*

From the analysis results, as shown in Figure 3 below, Smartphones had the highest (51.8%) index of device usage by respondents. Laptops and tablets also had a fair share among devices that MICK employees brought into the work place. This was an indicator of the emerging presence of portable devices in the workplace, owing to their functionalities (that they provided convenience, as well as a more personalized interface) that stretch beyond the traditional telephone calls and text messaging. Currently, statistics show that mobile devices are clear leaders in the list of the most significant security threats, as confirmed by security experts' study involving companies from various industries (Disterer & Kleiner, 2013).

| Device Owned | Responses | |
|---|---|---|
| | N | Percent |
| **Smartphone** | 71 | 51.8% |
| **Laptop** | 45 | 32.8% |
| **Tablet** | 15 | 10.9% |
| **Other** | 6 | 4.4% |
| **Total** | 137 | 100.0% |

***Figure 3: Devices owned and used at work***

### *4.2.2 Academic qualification versus device preference*

Further comparison of devices owned and the academic qualification of the respondents revealed that the use of Smartphones, which also happens to be the most prevalent device among the respondents, was highest among those with graduate level of education (76.1%). A similar trend was observed for laptops and tablets (80% of graduate employees) as depicted in Figure 4.

**Academic Qualification vs Device Preference**

| | | | Device Owned[a] | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Smartphone | Laptop | Tablet | Other | |
| Academic Qualification | Diploma | Count | 8 | 5 | 1 | 4 | 13 |
| | | % within $Device | 11.3% | 11.1% | 6.7% | 66.7% | |
| | | % of Total | 9.5% | 6.0% | 1.2% | 4.8% | 15.5% |
| | Graduate Degree | Count | 54 | 33 | 12 | 2 | 61 |
| | | % within $Device | 76.1% | 73.3% | 80.0% | 33.3% | |
| | | % of Total | 64.3% | 39.3% | 14.3% | 2.4% | 72.6% |
| | Post graduate Degree | Count | 8 | 7 | 2 | 0 | 9 |
| | | % within $Device | 11.3% | 15.6% | 13.3% | 0.0% | |
| | | % of Total | 9.5% | 8.3% | 2.4% | 0.0% | 10.7% |
| | Others | Count | 1 | 0 | 0 | 0 | 1 |
| | | % within $Device | 1.4% | 0.0% | 0.0% | 0.0% | |
| | | % of Total | 1.2% | 0.0% | 0.0% | 0.0% | 1.2% |
| Total | | Count | 71 | 45 | 15 | 6 | 84 |
| | | % of Total | 84.5% | 53.6% | 17.9% | 7.1% | 100.0% |

***Figure 4: Use/popularity of devices across education levels***

### *4.2.3 User knowledge of security threats in relation to devices*

Figure 5 displays levels of user awareness across three domains; knowledge of malware, patches/software updates and risks linked to use of portable devices on public Wi-Fi networks. Over half (59.5%) of the respondents did not know what malware was. Additionally, a significant proportion of respondents (61.9%) had knowledge of software updates/patches. More than half of the respondents (53.6%) had knowledge of the risks associated with use of portable devices in public Wi-Fi networks (hotspots).

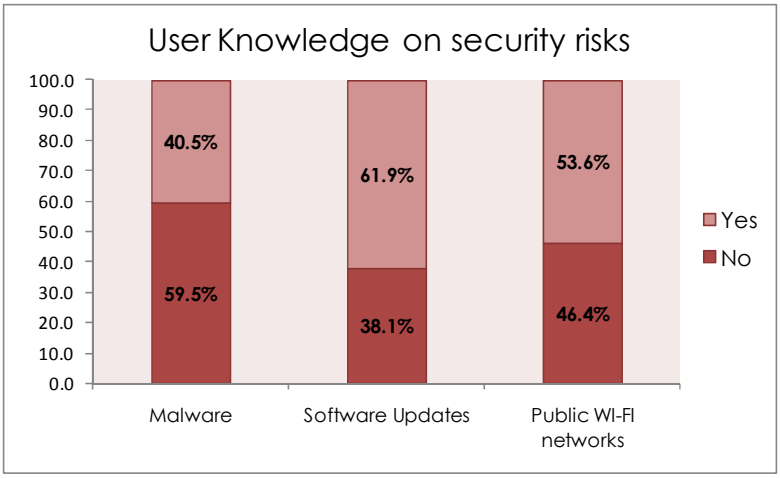



***Figure 6: User knowledge on security threat and risks***

### *4.2.4 User knowledge and installation of software updates/patches*

Probing further on the user knowledge and its application thereof, the analysis revealed that it was not habitual for those with the knowledge of software updates/patches to install software updates /patches. It was apparent from the results that installations of these updates happened by chance, that is, "sometimes" as indicated by the respondents (51.9%) in Figure 6.

***Figure 6: Knowledge of software updates/patches and user behavior***

| Knowledge of software updates/patches | | Installation of software updates/patches | | | | Total |
|---|---|---|---|---|---|---|
| | | Yes | sometimes | No | Not Applicable | |
| Yes | Count | 22 | 27 | 3 | 0 | 52 |
| | % within | 42.3% | 51.9% | 5.8% | 0.0% | 100.0% |
| | % of Total | 26.2% | 32.1% | 3.6% | 0.0% | 61.9% |
| No | Count | 0 | 0 | 0 | 32 | 32 |
| | % within | 0.0% | 0.0% | 0.0% | 100.0% | 100.0% |
| | % of Total | 0.0% | 0.0% | 0.0% | 38.1% | 38.1% |
| Total | Count | 22 | 27 | 3 | 32 | 84 |
| | % of Total | 26.2% | 32.1% | 3.6% | 38.1% | 100.0% |

As indicated in Figure 7, a majority (63.6%) of the respondents who did installation of updates/patches relied on computer or relatable prompting. It could be inferred that, a majority of them would not have installed these updates/patches (unless prompted) as some software do have an option of disabling update prompts, of which some software have updates turned off as their default setting. More so, users did have the option of disabling update prompts. That said however, it was notable that a fair share of the respondents (36.4%) who indeed installed the patches made an effort to search through the internet for the same.

*Figure 7: Frequency of software updates/patches installation*

| | | Frequency of installation | | | | |
|---|---|---|---|---|---|---|
| Does user install patches | | When prompted by the computer | I search through the internet and install | Never | Not Applicable | Total |
| Yes | Count | 14 | 8 | 0 | 0 | |
| | % within | 63.6% | 36.4% | 0.0% | 0.0% | 22 |
| | % of Total | 16.7% | 9.5% | 0.0% | 0.0% | 26.2% |
| Sometimes | Count | 22 | 5 | 0 | 0 | 26.2% |
| | % within | 81.5% | 18.5% | 0.0% | 0.0% | 27 |
| | % of Total | 26.2% | 6.0% | 0.0% | 0.0% | 32.1% |
| No | Count | 0 | 0 | 3 | 0 | 32.1% |
| | % within | 0.0% | 0.0% | 100.0% | 0.0% | 3 |
| | % of Total | 0.0% | 0.0% | 3.6% | 0.0% | 3.6% |
| Not Applicable | Count | 0 | 0 | 0 | 32 | 3.6% |
| | % within | 0.0% | 0.0% | 0.0% | 100.0% | 32 |
| | % of Total | 0.0% | 0.0% | 0.0% | 38.1% | 38.1% |
| Total | Count | 36 | 13 | 3 | 32 | 38.1% |
| | % of Total | 42.9% | 15.5% | 3.6% | 38.1% | 100.0% |

## 4.3 User Behavioral Trends

### *4.3.1 Use of devices in public hotspots*

As shown in Figure 8, majority (83.3%) of users agreed that they plugged their devices into public networks (wired or wireless). Public networks included home, malls, coffee shops, and restaurant hotspots. This user behavior was a noteworthy concern with regard to confidentiality and integrity elements around which BYOD data security concerns revolve (Keyes, 2014). A probable risk involved here was that an attacker would pry over the owner of a device with the intent of espying sensitive data or acquiring the devices password as it was being input.

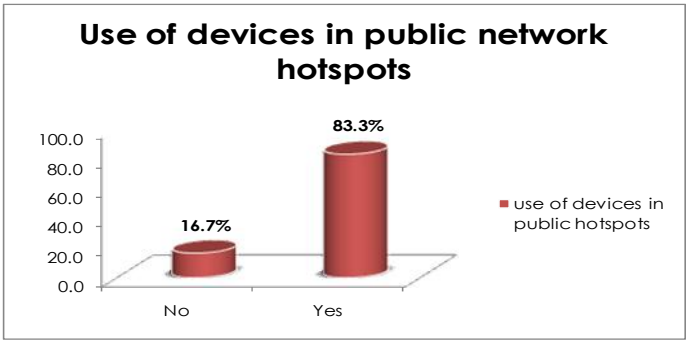



*Figure 8: Usage of wired or wireless networks*

Protection against threats for devices accessing public networks was also assessed. In Figure 9 below, it was evident that a majority of users had antivirus installations in their devices.

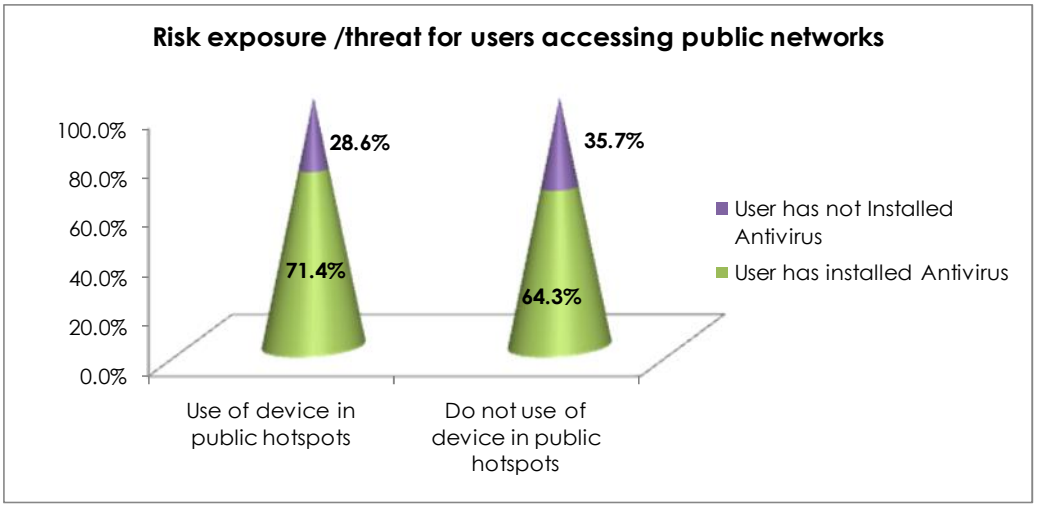



***Figure 9: Protection levels for devices assessing public network***

### *4.3.2 General level of device protection*

Further on user behavior, the level of device protection/exposure to threats was reported to be moderate. Asked if they had antivirus software installation in their devices, 48.8% of users agreed to the affirmative, out of those users, 69.5% had their antivirus up-to-date. An equal proportion (15.3%) did not have their antivirus up-to-date and also (15.3%) did not know if their antivirus was up-to-date, as tabulated in Figure 10 below. As earlier discussed, when people use mobile devices over wireless networks, there is usually a chance that the data being exchanged through the network can be accessed by an unauthorized third party (Mendez,2012). The analysis results indicated a commendable practice being exercised, that is, the installation of antivirus software. This however was only one facet of protection that may not cover all vulnerabilities associated with public networks.

| | | | Is Anti-virus upto date | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Yes | No | I dont know | Not applicable | |
| Anti-virus installed in device | Yes | Count | 41 | 9 | 9 | 0 | 59 |
| | | % within | 69.5% | 15.3% | 15.3% | 0.0% | 100.0% |
| | | % of Total | 48.8% | 10.7% | 10.7% | 0.0% | 70.2% |
| | No | Count | 0 | 2 | 2 | 21 | 25 |
| | | % within | 0.0% | 8.0% | 8.0% | 84.0% | 100.0% |
| | | % of Total | 0.0% | 2.4% | 2.4% | 25.0% | 29.8% |
| Total | | Count | 41 | 11 | 11 | 21 | 84 |
| | | % of Total | 48.8% | 13.1% | 13.1% | 25.0% | 100.0% |

***Figure 10: General level of device protection***

### *4.3.2 Level of protection against unauthorized access to devices*

Users were requested to pick the unauthorized access security they used in their devices. Figure 11 below shows percentages of security measures employed to protect devices. Passwords were the most frequently (41%) used of the four (4) security measures assessed. PIN codes followed closely (32.7%), while biometrics was the least used (1.3%). It should also be noted that there was still a proportion (albeit small, 3.6%) of the users who did not have any security measures in their devices.

| | | Responses | |
|---|---|---|---|
| | | N | Percent |
| Security Measures | PIN Codes | 51 | 32.7% |
| | Passwords | 64 | 41.0% |
| | Biometrics | 2 | 1.3% |
| | Pattern Codes | 36 | 23.1% |
| | None | 3 | 1.9% |
| | Total | 156 | 100.0% |

***Figure 11: Access Security Measures***

### *4.3.3 User password strengths*

A follow up on the passwords in particular, revealed that a majority (47.6%) have their passwords comprising of combination of texts, numerals and special characters such as commas, asterisks, harsh et cetera. This was an indication of use of strong passwords. This is depicted in Figure 12 below.

| What comprises your passwords | Frequencies | |
|---|---|---|
| | Count | Valid Percent |
| **Combination of texts, numerals and special characters such as commas, asterisks, harsh etc** | 40 | 47.6% |
| **Plain numerals less than seven digits** | 18 | 21.4% |
| **Plain texts of more than seven characters** | 9 | 10.7% |
| **Plain tests less than seven characters** | 7 | 8.3% |
| **Plain numerals more than seven digits** | 6 | 7.1% |
| **Not applicable** | 4 | 4.8% |
| **Total** | 84 | 100.0 |

***Figure 12: Strength of passwords used***

### *4.3.4 Frequency of change in security measures*

As shown in Figure 13, whilst most of the users had security measures in place, a majority (41.7%) of them never actually updated or changed them. The concern of confidentiality therefore arose; confidentiality is a data security element that ensures that the data/information being relayed cannot be read by unauthorized entities. Use of strong passwords as well as frequent change of the same usually guaranteed some level of data security with regard to confidentiality. In effect, passwords guarantee data integrity which involves detection of any changes that are made on transmitted data (whether intentional or unintentional).

| | | Frequency | Valid Percent |
|---|---|---|---|
| How often do you change password | Never | 35 | 41.7 |
| | Every 3 months | 31 | 36.9 |
| | Every Year | 7 | 8.3 |
| | Every 9 months | 2 | 2.4 |
| | Every 6 months | 9 | 10.7 |
| | Total | 84 | 100.0 |

***Figure 13: Frequency change of security measures***

### *4.3.5 Ratio of people sharing security codes*

Figure 14 below shows the proportion of users who shared their devices security code and compared the proportion of users that changed the security code thereafter. 61.9% shared the devices with at least one person but did not change the security measures thereafter. The rudimentary virtues of authenticity, confidentiality and integrity are those that were faced with the greatest threat of compromise here. With regard to confidentiality, a peril arose when unauthorized parties obtained access to material that was classified. This was achieved through either intercepting data transmissions or manipulating devices. Manipulation is usually performed by utilizing inadequately secured devices which in effect threatens the confidentiality of corporate data (Disterer & Kleiner, 2013).

| | | Approximate number people the user has shared security code with | | | | | |
|---|---|---|---|---|---|---|---|
| | | One person | Two people | Three people | More than three people | NA | Total |
| Did you thereafter change security code after sharing it? | Yes | 8 | 7 | 4 | 1 | 0 | 20 |
| | | 38.1% | 58.3% | 80.0% | 16.7% | 0.0% | 23.8% |
| | No | 13 | 5 | 1 | 4 | 0 | 23 |
| | | 61.9% | 41.7% | 20.0% | 66.7% | 0.0% | 27.4% |
| | Not Applicable | 0 | 0 | 0 | 1 | 40 | 41 |
| | | 0.0% | 0.0% | 0.0% | 16.7% | 100.0% | 48.8% |
| Total | | 21 | 12 | 5 | 6 | 40 | 84 |
| | | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% |

***Figure 14: Change of security codes after sharing it***

### *4.3.6 Trouble- shooting of devices*

As observed by Disterer & Klein (2013), there arises the need for assistance by users in installing software and the registration of privately owned devices. Albeit the inherent risk, the greatest proportion (64.3%) of respondents was, according to this study, comfortable with getting assistance from a third party (colleague, friend or someone they consider IT savvy) as graphed in Figure 15. This finding revealed a gap in user behavior that exposed the company to the threat of unauthorized access to confidential information or data that the assisting third party was not privy to.

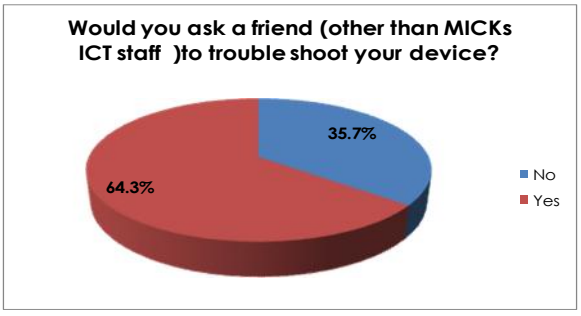



***Figure 15: Assistance on trouble shooting devices***

## 4.4 Hypothesis Testing and Inferential Statistics

### *4.4.1 Hypothesis*

In order to perform significance test to decide whether, based upon the sample of users drawn from the company, there is any or no evidence to suggest that linear correlation is present in the population, we test the null hypothesis.

Ho: There was no correlation between risky BYOD user behavior and information insecurity within the organization.

This was tested against the alternative hypothesis:

$H_1$: There was a correlation between risky BYOD user behavior and information insecurity within the organization

The researcher's empirical basis in formulating the hypotheses was that the lack of a BYOD adoption policy for MICK employees had encouraged certain dangerous BYOD user behaviors to thrive. These behavioral outcomes were evaluated through two perspectives namely (i) Assessment the levels of user awareness on matters relating to BYODs; and (ii) BYOD user behavioral attributes which encouraged information insecurity.

### *4.4.2 Inferential Statistics*

Measure of association was done using the Spearman rank-order correlation. The Spearman rank-order correlation coefficient (Spearman's correlation, for short) is a non-parametric measure of the strength and direction of association that exists between two variables measured on at least an ordinal scale (Hauke & Kossowski, 2011). Specifically, Spearman's correlation coefficient is a statistical measure of the strength of a monotonic relationship between paired data. Hauke & Kossowski (2011) further explain that a monotonic function is one that either never increases or never decreases as its independent variable increases. The correlation coefficient is denoted by $r_s$ (or the Greek letter ρ, pronounced rho) and its values range from -1 to 1, interpretation being that the closer $r_s$ is to +1 the stronger the monotonic relationship. As stated by Hauke & Kossowski (2011), "this test is used for either ordinal variables or for continuous data that has failed the assumptions necessary for conducting the Pearson's product-moment correlation" used otherwise for used for nominal variables.

According to Huck (2012), determination whether a relationship exists between two different variables and the establishment of the significance or strength of the association between the two variables is

useful. The strength of the correlation is not dependent on the direction or the sign. For instance, r = 0.90 and r = -0.90 are equal in the degree of association of the measured variables (Huck, 2012). A positive correlation coefficient indicates that an increase in the first variable would correspond to an increase in the second variable, thus implying a direct relationship between the variables (Huck, 2012). A negative correlation indicates an inverse relationship whereas one variable increases the second variable decreases.

Significance of correlation is ascertained if the sample correlation is so large that it is likely to occur by chance say only 5 (5%) times in a hundred tries (it has a $p < .05$), it is assumed that it reflects a genuine correlation in the population from which the sample came from (Huck, 2012).

The data drawn from the survey was in ordinal measure and was deemed perfect for this analysis.

i. User academic qualification and preferred choice of device (Do these two have any correlation or other factors such income come into play?)
ii. Association between user awareness and user behavior (Does user awareness levels have bearing on user behavior?).
iii. User age and user behavior (Are there any correlations between user age and user behavior?)

### *a. Academic qualification and choice of device(s)*

| | | | Academic Q |
|---|---|---|---|
| Spearman's rho | Academic Q | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 84 |
| | Smartphone | Correlation Coefficient | .226* |
| | | Sig. (2-tailed) | .038 |
| | | N | 84 |
| | Laptop | Correlation Coefficient | .160 |
| | | Sig. (2-tailed) | .145 |
| | | N | 84 |
| | Tablet | Correlation Coefficient | .091 |
| | | Sig. (2-tailed) | .411 |
| | | N | 84 |
| | Others | Correlation Coefficient | -.339** |
| | | Sig. (2-tailed) | .002 |
| | | N | 84 |

*Table 2: Correlations between choice of device and academic qualification*

A Spearman's correlation was run to determine the relationship between devices owned and used by staff in the office and their academic qualification. As tabulated in *Table 1*, there was a statistically significant positive correlation between Smartphone ownership and academic qualification (= .226, n = 84, p < .05) as well as a statistically significant negative correlation between other devices and academic qualification (= -.339, n = 84, p < .05). It was also noted that the correlations in both cases was moderately weak, looking at the correlation coefficients. The other devices had a positive correlation with academic qualification; the relationship was not statistically significant at 5% level of significance.

### *b. Academic qualifications and user behaviors*

**Correlations**

| | | | AcademicQ | QB1 | QB2 | QB3 | QB4 | QB5 | QB8 | QB9 | QB11 | QB12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Spearman's rho | AcademicQ | Correlation Coefficient | 1.000 | -.276* | -.010 | -.149 | -.052 | -.018 | -.087 | .117 | .090 | -.042 |
| | | Sig. (2-tailed) | . | .011 | .926 | .176 | .641 | .872 | .433 | .290 | .415 | .705 |
| | | N | 84 | 84 | 84 | 34 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB1 | Correlation Coefficient | -.275* | 1.000 | .058 | .091 | -.205 | .137 | .079 | .128 | .079 | .000 |
| | | Sig. (2-tailed) | .011 | . | .599 | .412 | .061 | .215 | .476 | .247 | .477 | 1.000 |
| | | N | 84 | 84 | 84 | 34 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB2 | Correlation Coefficient | -.010 | .058 | 1.000 | .811** | .022 | .095 | .215* | .130 | .153 | -.050 |
| | | Sig. (2-tailed) | .926 | .599 | . | .000 | .843 | .389 | .050 | .238 | .164 | .649 |
| | | N | 84 | 84 | 84 | 34 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB3 | Correlation Coefficient | -.149 | .091 | .811** | 1.000 | -.037 | .052 | .255* | .079 | .101 | -.029 |
| | | Sig. (2-tailed) | .176 | .412 | .000 | . | .738 | .636 | .019 | .474 | .359 | .796 |
| | | N | 84 | 84 | 84 | 34 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB4 | Correlation Coefficient | -.052 | -.205 | .022 | -.037 | 1.000 | .144 | .160 | .024 | .042 | -.126 |
| | | Sig. (2-tailed) | .641 | .061 | .843 | .738 | . | .190 | .147 | .827 | .707 | .253 |
| | | N | 84 | 84 | 84 | 34 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB5 | Correlation Coefficient | -.018 | .137 | .095 | .052 | .144 | 1.000 | .002 | .071 | .078 | .206 |
| | | Sig. (2-tailed) | .872 | .215 | .389 | .636 | .190 | . | .983 | .520 | .480 | .060 |
| | | N | 84 | 84 | 84 | 34 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB8 | Correlation Coefficient | -.087 | .079 | .215* | .255* | .160 | .002 | 1.000 | .031 | .074 | -.353** |
| | | Sig. (2-tailed) | .433 | .476 | .050 | .019 | .147 | .983 | . | .780 | .502 | .001 |
| | | N | 84 | 84 | 84 | 34 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB9 | Correlation Coefficient | .117 | .128 | .130 | .079 | .024 | .071 | .031 | 1.000 | .905** | .099 |
| | | Sig. (2-tailed) | .290 | .247 | .238 | .474 | .827 | .520 | .780 | . | .000 | .368 |
| | | N | 84 | 84 | 84 | 34 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB11 | Correlation Coefficient | .090 | .079 | .153 | .101 | .042 | .078 | .074 | .905** | 1.000 | .063 |
| | | Sig. (2-tailed) | .415 | .477 | .164 | .359 | .707 | .480 | .502 | .000 | . | .567 |
| | | N | 84 | 84 | 84 | 34 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB12 | Correlation Coefficient | -.042 | .000 | -.050 | -.029 | -.126 | .206 | -.353** | .099 | .063 | 1.000 |
| | | Sig. (2-tailed) | .705 | 1.000 | .649 | .736 | .253 | .060 | .001 | .368 | .567 | . |
| | | N | 84 | 84 | 84 | 34 | 84 | 84 | 84 | 84 | 84 | 84 |

*. Correlation is significant at the 0.05 level (2-tailed).

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

*Table 2: Correlations between academic qualification and user behavior*

There is negative statistically significant (at 5% level of significant, P<.05) correlation between academic qualification and use of device(s) on other wired or wireless networks (hotspots) such as

coffee shops, restaurants, at home. With higher academic qualification, user behavior seems to be changing; academic qualification and variable B1. The other user behaviors compared to academic qualifications have an association to some extent but the same was not statistically significant.

### *c. Correlation between devices owned and the use of devices on wired or wireless networks (public Wi-Fi)*

| Correlations | | | |
|---|---|---|---|
| | | | Use of device on public wireless networks |
| Spearman's rho | Use of device on wireless networks | Correlation Coefficient | 1.000 |
| | | Sig. (2-tailed) | . |
| | | N | 84 |
| | Laptop | Correlation Coefficient | -.224* |
| | | Sig. (2-tailed) | .040 |
| | | N | 84 |
| | Smartphone | Correlation Coefficient | -.074 |
| | | Sig. (2-tailed) | .506 |
| | | N | 84 |
| | Tablet | Correlation Coefficient | -.042 |
| | | Sig. (2-tailed) | .706 |
| | | N | 84 |
| | Other devices | Correlation Coefficient | .000 |
| | | Sig. (2-tailed) | 1.000 |
| | | N | 84 |

*Table 3: Correlations between devices owned and the use of devices on wired or wireless networks (public Wi-Fi)*

Of all the devices, only laptops had a significant correlation (though weak; = -.224, n=84, p<.05) with use on public Wi-Fi. The association was negative to mean that laptops owned by staff were less likely to be used or were being used in a decreasing frequency on public places compared to other devices.

### *d. Knowledge of malware and installation of antivirus*

**Correlations**

| | | | Do you understand malware | Do you have anti-virus installed in your device |
|---|---|---|---|---|
| Spearman's rho | Do you understand malware | Correlation Coefficient | 1.000 | .229* |
| | | Sig. (2-tailed) | . | .036 |
| | | N | 84 | 84 |
| | Do you have anti-virus installed in your device | Correlation Coefficient | .229* | 1.000 |
| | | Sig. (2-tailed) | .036 | . |
| | | N | 84 | 84 |

*. Correlation is significant at the 0.05 level (2-tailed).

*Table 4: Correlations between knowledge of malware and installation of antivirus*

There was a positive significant (at 5% level of significance, $p < .05$) association between knowledge and behavior; those with the knowledge of the threat of malware had their devices installed with anti-virus software, again it could be remarked that those without the knowledge were likely to have no antivirus installed in their devices.

**Correlations**

| | | | Q2 | QB1 | QB4 | QB5 |
|---|---|---|---|---|---|---|
| Spearman's rho | Q2 | Correlation Coefficient | 1.000 | .096 | -.133 | .042 |
| | | Sig. (2-tailed) | . | .385 | .227 | .706 |
| | | N | 84 | 84 | 84 | 84 |
| | QB1 | Correlation Coefficient | .096 | 1.000 | -.205 | .137 |
| | | Sig. (2-tailed) | .385 | . | .061 | .215 |
| | | N | 84 | 84 | 84 | 84 |
| | QB4 | Correlation Coefficient | -.133 | -.205 | 1.000 | .144 |
| | | Sig. (2-tailed) | .227 | .061 | . | .190 |
| | | N | 84 | 84 | 84 | 84 |
| | QB5 | Correlation Coefficient | .042 | .137 | .144 | 1.000 |
| | | Sig. (2-tailed) | .706 | .215 | .190 | . |
| | | N | 84 | 84 | 84 | 84 |

Q2: Do you understand security risks of using your device(s) on public Wi-Fi networks

QB1: Do you use your device(s) on other wired or wireless networks (hotspots) such as coffee shops, restaurants, at home?

QB4: Do you store company data (emails correspondences, file attachments etc) on your portable devices?

QB5: Could someone else access your data if your Smartphone/laptop/tablet were stolen right now?

Compared together, these variables had an association (both in positive and negative direction) but the same association was not significant at the 5% level of significance. Meaning whilst it was evident that there was a level of association between the user knowledge (in the areas assessed) and the behavior in the same areas, the association was not significant and this could not be due to chance.

### *e. Knowledge and threat of Sharing Devices*

**Correlations**

| | | | Q2 | QB8 | QB9 | QB11 |
|---|---|---|---|---|---|---|
| Spearman's rho | Q2 | Correlation Coefficient | 1.000 | .202 | .072 | .051 |
| | | Sig. (2-tailed) | . | .065 | .517 | .647 |
| | | N | 84 | 84 | 84 | 84 |
| | QB8 | Correlation Coefficient | .202 | 1.000 | .031 | .074 |
| | | Sig. (2-tailed) | .065 | . | .780 | .502 |
| | | N | 84 | 84 | 84 | 84 |
| | QB9 | Correlation Coefficient | .072 | .031 | 1.000 | .905** |
| | | Sig. (2-tailed) | .517 | .780 | . | .000 |
| | | N | 84 | 84 | 84 | 84 |
| | QB11 | Correlation Coefficient | .051 | .074 | .905** | 1.000 |
| | | Sig. (2-tailed) | .647 | .502 | .000 | . |
| | | N | 84 | 84 | 84 | 84 |

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

*Table 5: Correlations between knowledge and threat of sharing devices*

Q2: Do you understand security risks of using your device(s) on public Wi-Fi networks

QB8: How often do you change your security measures?

QB9: Have you ever shared your devices passwords?

QB11: Did you change password after sharing?

Compared together, these variables had an association (positive and negative) but the same association was not significant at the 5% level of significance. Meaning, while it was evident that there was a level of association between the user knowledge (in the areas assessed) and the behavior in the same areas, the association was not significant and this could not be occasioned to probability.

### *f. Correlation between Age and user behavior*

**Correlations**

| | | | Age | QB1 | QB2 | QB3 | QB4 | QB5 | QB8 | QB9 | QB11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Spearman's rho | Age | Correlation Coefficient | 1.000 | -.009 | -.051 | -.063 | -.434** | -.116 | -.086 | .035 | .033 |
| | | Sig. (2-tailed) | . | .936 | .643 | .568 | .000 | .295 | .437 | .751 | .763 |
| | | N | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB1 | Correlation Coefficient | -.009 | 1.000 | .058 | .091 | -.205 | .137 | .079 | .128 | .079 |
| | | Sig. (2-tailed) | .936 | . | .599 | .412 | .061 | .215 | .476 | .247 | .477 |
| | | N | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB2 | Correlation Coefficient | -.051 | .058 | 1.000 | .811** | .022 | .095 | .215* | .130 | .153 |
| | | Sig. (2-tailed) | .643 | .599 | . | .000 | .843 | .389 | .050 | .238 | .164 |
| | | N | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB3 | Correlation Coefficient | -.063 | .091 | .811** | 1.000 | -.037 | .052 | .255* | .079 | .101 |
| | | Sig. (2-tailed) | .568 | .412 | .000 | . | .738 | .636 | .019 | .474 | .359 |
| | | N | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB4 | Correlation Coefficient | -.434** | -.205 | .022 | -.037 | 1.000 | .144 | .160 | .024 | .042 |
| | | Sig. (2-tailed) | .000 | .061 | .843 | .738 | . | .190 | .147 | .827 | .707 |
| | | N | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB5 | Correlation Coefficient | -.116 | .137 | .095 | .052 | .144 | 1.000 | .002 | .071 | .078 |
| | | Sig. (2-tailed) | .295 | .215 | .389 | .636 | .190 | . | .983 | .520 | .480 |
| | | N | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB8 | Correlation Coefficient | -.086 | .079 | .215* | .255* | .160 | .002 | 1.000 | .031 | .074 |
| | | Sig. (2-tailed) | .437 | .476 | .050 | .019 | .147 | .983 | . | .780 | .502 |
| | | N | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB9 | Correlation Coefficient | .035 | .128 | .130 | .079 | .024 | .071 | .031 | 1.000 | .905** |
| | | Sig. (2-tailed) | .751 | .247 | .238 | .474 | .827 | .520 | .780 | . | .000 |
| | | N | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 |
| | QB11 | Correlation Coefficient | .033 | .079 | .153 | .101 | .042 | .078 | .074 | .905** | 1.000 |
| | | Sig. (2-tailed) | .763 | .477 | .164 | .359 | .707 | .480 | .502 | .000 | . |
| | | N | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 | 84 |

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

*. Correlation is significant at the 0.05 level (2-tailed).

*Table 6: Correlations between age and user behavior*

Q2: Do you understand security risks of using your device(s) on public Wi-Fi networks

QB1: Do you use your device(s) on other wired or wireless networks (hotspots) such as coffee shops, restaurants, at home?

QB2: Do you have an anti-virus installed in your device?

QB3: Is your anti-virus application up to date?

QB4: Do you store company data (emails correspondences, file attachments etc) on your portable devices?

QB5: could someone else access your data if your Smartphone/laptop/tablet were stolen right now?

QB8: How often do you change your security measures?

QB9: Have you ever shared your devices passwords?

QB11: Did you change password after sharing?

Age and storage of company information in user/staff devices appeared to have a significant negative association at 5% level of significance ($p<.05$), translated to imply that with increase in age and consequently responsibilities at the place of work, analysis results revealed that there was an increase in negative user behavior. The negative user behavior here was that 'older' users stored company details in their devices the most (arguably so that they could still continue working after work or outside the office environment). For the other variables compared together, majority of these variables had an association (positive and negative) but the same association was not significant at the 5% level of significance as displayed in figure 4. Meaning, whilst it was evident that there was a level of association between user knowledge (in the areas assessed) and the behavior (in the same areas) the association was not significant, that is, it could not be occasioned to probability.

### 4.5 Hypothesis testing and conclusion

The null hypothesis being tested was as follows:

Ho: $r_s = 0$

Against the alternative hypothesis;

$H_1 : r_s \neq 0$

From the analysis results (as discussed in the inferential statistics section), for a majority of the variables on user behavior and trends as well as user demographic characteristics the correlation coefficients were different from zero (0). The null hypothesis is thus rejected in favor of the alternative hypothesis. Testing the statistical significance of the correlation between the variables at the 5% level of significance reveals that whilst a most of correlations were not statistically significant there was found to be a weak-to-moderately strong but statistically significant correlation between some aspects of user knowledge of security threats/vulnerabilities, user behavior scores and user demographic attributes (age and academic qualification). For instance, of all the devices owned and used at work by staff, only laptops had a significant correlation with use on public Wi-Fi. The negative association can be inferred to mean that laptops owned by staff are less likely to be used or are being used in a decreasing frequency on public places compared to other devices. Correlation between user age and storage of company information in own devices was found to have a significant moderately strong

negative association at 5% level of significance, translated to infer that with increase in age (and same to responsibilities at the place of work) the behavior is that users are more prone to store company details in their devices (possibly to still keep working after work or outside the office environment). A positive significant association was reported between knowledge and behavior; for instance those with the knowledge of the threat of malware have their devices installed with anti-virus software, again it can be remarked that those without the knowledge are likely to have no antivirus installed in their devices. Other aspects of user knowledge, awareness and user behavior were reported to have an extent of association but the same was not significant at the 5% level of significance.

### 4.6 Expert's opinion on BYOD

A similar (containing same aspects of security threats and risks as the employees survey) questionnaire was administered to MICK ICT experts seeking their opinion on an array of issues relatable to BYOD.

#### 4.6.1 User behavior, challenges thereof and concerns

Regarding MICK agents using BYODs, what concerned MICK's ICT team the most was a tie between data security and compliance. Additionally, what they considered to be BYODs threat to information security, a majority cited the threat posed by viruses. The argument was that these devices do not have antivirus protection which makes the same devices vulnerable to viruses hence a threat to MICK network. They felt there was need to continuously run software updates, install anti-virus software, restrict/block access to certain websites, limit access to certain employees, and even incorporate passwords/PINs.

Expertise advice and recommendations to their employees was majorly on importance of running updates, the need to report data security issues urgently, importance of changing passwords and PINs regularly, importance of accessing information when on secure networks (for example, those that required passwords) as well as the importance of encrypting messages to protect sensitive information. Asked whether MICK had a formal BYOD policy, they reported that this was not available, and as such they pointed out the need for such a policy particularly to cover aspects such as protection for employees in relation to privacy and loss of personal information, back-up and recovery of personal data (if an employee lost or inadvertently wiped their mobile device) and back-up and restore of personal data if their mobile device was hacked. Majority agreed that the benefits of a BYOD policy somewhat outweighed the risks thereof. The consensus among the experts was that the primary

responsibility of keep employee's personal mobile devices secure when they were accessing company information or applications lied with both the employee and the organization.

### 4.7 Conclusion

In a nutshell, the study revealed that the rudimentary aspects of confidentiality, integrity and authenticity were the ones that were faced with the greatest threat of compromise in MICK, for example, the greatest proportion (64.3%) of users, according to the study, were comfortable with getting IT assistance from a third party other than an IT staff (e.g. a colleague or friends outside the office) but this cannot be directly linked to the lack of a BYOD policy in the company. Study findings further revealed that users were not aware of the great importance of ensuring information security. Majority of users (83.3%) agreed to docking their devices onto public networks (wired or wireless). These public networks included home, malls, coffee shops, and restaurant hotspots. This user behavior is a noteworthy concern with regard to confidentiality and integrity elements around which BYOD data security concerns revolve (Keyes 2014). A probable risk involved here is that an attacker would pry over the owner of a device with the intent of espying sensitive data or acquiring the devices password as it is being input. The implications here pose grave security gaps because MICK's data will be stored and transmitted using devices and networks which the employer does not own or manage so in the case where the has no adequate protection mechanism, privacy and security risks are posed to the safety of the company's trade secret, proprietary, or confidential information. The privacy and security of sensitive personal data is also exposed.

Confidentiality is a considerable data security element that ensures that the data/information being relayed cannot be read by unauthorized entities. The use of strong password passwords and frequently changing them usually guarantees a certain level of data security with regard to confidentiality. From the MICK study, confidentiality concerns arose in relation to use of passwords. The study findings revealed that although a majority (47.6%) of users have their passwords comprising of combination of texts, numerals and special characters such as commas, asterisks, harsh et cetera; an indication of use of strong passwords) as well as frequent change of the same, out of the 84 users polled, the majority (41.7%) never changed their passwords thus underpinning the confidentiality concern. Again, password sharing among users was very common and most users who shared passwords did not change them thereafter. It is worth noting that in effect, passwords guarantee data integrity which involves detection of any changes that are made on transmitted data (whether intentional or unintentional).

Irrefutably, as the evidenced user BYOD behavior at MICK presents some significant level of information insecurity concern, it can be concluded that MICK needs to have a BYOD framework and policy put in place and its staff need continuous sensitization on matters pertaining the BYOD phenomenon so as to foster information security at the organization.

### 4.8 Adoption of a BYOD model for MICK

The analysis results revealed commendable degree of user knowledge on information security and consequently the threats/vulnerabilities posed to the company were found to be considerably low. Additionally, it was inferred that a high likelihood of an influx of user owned devices into the work place was inevitable hence a foreseeable growth in data and information security threats. Relating these results to the adoption of a befitting BYOD model for the company, it is an interesting discovery that the environment at MICK is ripe for the Optimized Hybrid conceptual framework for BYOD adoption. The attractiveness of this type of a model, and its agreeability with the study findings, is the flexibility and the fact that it takes into consideration the underlying organizations infrastructure (Mwenemeru & Omwenga, 2014). This way, since the company does not have in place a BYOD policy, the current ICT policy and infrastructure will anchor the model then a build up to the BYOD policy can be done phase-wise.

The hybrid framework has its features from combinations of four other categories of models. An example of adoption could be "Users can use any device with wireless capability to connect to the organizations network provided that the user has a login account and agrees to behave as stipulated on the ICT policy" (Alberta, 2006). The advantages and disadvantages of the hybrid model vary according to the combination (hybrid) chosen. In the words of Khanna (2013), while 91% of businesses consider data security to be their number one IT priority, 21% of businesses do not have a policy to safeguard against data sharing across consumer-grade platforms; this is a contradiction because figures reveal that many data breaches as resultant of internal laxity over data control (Khanna, 2013). The Optimized Hybrid conceptual framework can mitigate the disadvantages by bringing to the table a MDM application such as MaaS360 or 2x (which the organization lacks) to work hand-in-hand with a NAC such as domain controllers and McAfee ePO (which the organization already has in place).

### 4.8.1 Recommendation

This research has shown that BYOD information security threats exist at MICK, owing to aforementioned lax user behavior and to the anticipated growth in the use of BYODs. Consequently, MICK ICT infrastructure is ripe for a BYOD framework and policy. The policy should address the following areas of concern:

a. User awareness should be enforced through continuous sensitization of users on emerging threats associated with BYODs such as password sharing risks, importance of anti-virus software, the risks involved in using of devices in hotspots, the general importance of devices protection and importance of use of strong passwords/security measures.
b. ICT should be instrumental in giving direction and offering expert advice on policy matters that they feel the BYOD policy must address regarding emerging threats.
c. It is vital for the organization to acquire a Mobile Device Management (MDM) application so as to gain visibility of BYODs.
d. Checks be put in place to ensure portable devices have up-to-date anti-virus programs (as indicated by ICT, malware is the greatest threat concern).
e. Frequent and continuous training on current and emerging information security matters should be inculcated at MICK.

"Security today is about flexibility not rigidity" remarks Khanna (2013); in adopting these considerations for their BYOD model, the MICK IT department, suffice it to say, through the ICT policy, will wield the power to put in place solutions that are effective despite the fluid use of devices and technologies, "in a climate of 'bring-your-own-everything', reckons Khanna (2013).

### 4.8.9 Recommendation for Further Studies

For further investigation, this study proposes the following:

*Impact of not inventorying authorized and unauthorized BYOD access to an organization's network.*

BYODs can be used to perform mischievous activities that may be a detriment to organizational informational assets. In order to avert this threat, it is pertinent fot ICT departments to inventory both authorized and authorized accesses that BYODs have made on the network and take necessary action where breaches have been made.

*Exploration into user groups which should be allowed to use BYODs in organizations.*

In as much as BYODs bring perceived benefits for all users, not all organizations user groups should be allowed to use BYODs. Organizations should therefore define which groups of users should allowed to bring personal devices and segmenting these user groups in order to adopt a BYOD program that suits business needs.

*Impact of not vetting personal devices when employees join or leave an organization.*

The exits risks in allowing BYODs into the organization without vetting them for applications that may present threats to the organization. Similarly, when employees leave the organization, their personal devices ought to be checked for data which the organization feels must not leave the organization. Failure to vetting personal devices can have serious consequences on the organizations in form of industrial espionage which ICT departments need to deter.

## References


Allam, S., Flowerday, S.V. & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*. [Online] 42. pp. 56–65. Available from - http://www.sciencedirect.com/science/article/pii/S0167404814000169. [Accessed: May 01, 2014].

Antonopoulos, A. (2011). IT Security's Scariest Acronym: BYOD, bring your own device. *Network World*. [Online] Available from - http://www.networkworld.com/article/2179632/smartphones/it-security-s-scariest-acronym--byod--bring-your-own-device.html. [Accessed: June 29th, 2014]

Blythe, J.M., 2013. Cyber Security in the Workplace: Understanding and Promoting Behaviour Change., in *CHItaly (Doctoral Consortium)*. Trento (Italy) , Monday 16th September 2013. Trento: http://ceur-ws.org. pp. 1 - 10 .

Brandly, T. (2011). Pros and Cons of Bringing Your Own Device. *PCWorld*. [Online] 20th December, 2011). Available from - http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html. [Accessed: 15th June, 2014].

Canada. Alberta Government. (2012). *Bring Your Own Device: A Guide for Schools*. Alberta Education: Canada. [Online]. Available from - http://www.education.alberta.ca/media/6724519/byod%20guide%20final.pdf. [Accessed: July 19th 2014].

Creswell, J. W. (1998) *Qualitative inquiry and research design: Choosing among five traditions.* Thousand Oaks, CA: SAGE Publications.

Danford, T.E., Batchu, S.K., 2013. *Virtual instance architecture for mobile device management systems.* [Online] USA. Google Patents. Available from - http://www.google.com/patents/US8396465. [Accessed: July 17, 2014]

Disterer, G. & Kleiner C. (2013). BYOD Bring Your Own Device. *Procedia Technology.* [Online] Vol. 9. pp. 43 - 53. Available from - http://www.sciencedirect.com/science/article/pii/S22121731300159X [Accessed: 4th August,2014].

Hauke, J., & Kossowski, T. (2011). Comparison of values of Pearson's and Spearman's correlation coefficient on the same sets of data. *Quaestiones Geographicae.* [Online] 30 (2). pp. 87–93. Available from - http://geoinfo.amu.edu.pl/qg/archives/2011/QG302_087-093.pdf [Accessed: November 2nd, 2014].

Huck, S.W. (2012). Reading statistics and research (6th ed). Boylston Street, Boston, MA: Pearson Education.

Johnson, S. (2013) Bringing IT out of the shadows. *Network Security*. [Online] 2013 (12). pp. 5–6. Available from - www.sciencedirect.com/science/article/pii/S135348581370134X. [Accessed: July 5th 2014].

Keyes, J. (2014) *BYOD for Healthcare*. [Online] Boca Raton FL: Auerbach. Available from http://www.ebooks-share.net/byod-for-healthcare/. [Accessed: September 4th 2014].

Khanna, R. (2013) Data breaches: the enemy within. *Computer Fraud & Security.* [Online] 2013 (8). pp. 8–11. Available from - http://www.sciencedirect.com/science/article/pii/S136137231370071X. [Accessed: September 5th 2014]

Kulkarni, G. et al (2014). Mobile Cloud Computing - Bring Your Own Device. In - *Fourth International Conference on Communication Systems and Network Technologies (CSNT).* Bhopal, Monday 7th to Wednesday 9th April, 2014. Bhopal: IEEE. pp. 565–568.

Maniscalchi, J. (2009). Threat vs Vulnerability vs Risk. [Online] June 26th 2009. Available from - http://www.digitalthreat.net/2009/06/threat-vs-vulnerability-vs-risk/#. [Accessed: 12th October, 2014]

Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. *Computer Fraud & Security*. [Online] 2012 (14). pp. 14–17. Available from - http://www.sciencedirect.com/science/article/pii/S1361372312700313. [Accessed: July 5th 2014].

Mendez, A.(2012) *BYOD Technology*. Unpublished.

Morrow, B. (2012) BYOD security challenges: control and protect your most sensitive data. *Network Security*. [Online] 2012 (12). pp. 5–8. Available from - www.sciencedirect.com/science/article/pii/S1353485812701113. [Accessed: July 5th 2014].

Mugenda,A. & Mugenda, O. (2003) Research Methods: Quantitative and Qualitative Approaches. Nairobi: African Centre for Technology Studies (ACTS).

Mwenemeru, H. K. & Omwenga, V. O. (2014) Towards the adoption of bring_your_own_device concept in an organization. *International Journal of Social Sciences and Entrepreneurship*, 1 (11). pp. 534-546.

Niharika, S. (2012) B.Y.O.D Genie Is Out Of the Bottle – "Devil Or Angel". *Journal of business management & social sciences research (JBM&SSR)*. [Online] 1(3). Available from - www.borjournals.com/Research_papers/Dec_2012/1060%20%20M.pdf. [Accessed: July 5th 2014].

Pham, D. et al. (2005). Secure Network File Access Controller Implementing Access Control and Auditing. US Patents Patent no. US 6931530 B2 [Online]. Available from: www. google.com/patents/US6931530 [Accessed: January 17th 2015].

Pillay, A. et al. (2013) Does BYOD increase risks or drive benefits? *The University of Melbourne.* [Online] 2013. Available from - https://minerva-access.unimelb.edu.au/bitstream/handle/11343/33345/300314_2013_Tan_Risk.pdf?sequence=1. [Accessed: June 25th 2014].

Romer, H. (2014) Best practices for BYOD security. *Computer Fraud & Security*. [Online] 2014 (1). Available from - http://www.sciencedirect.com/science/article/pii/S1361372314700077. [Accessed: June 20th 2014].

Stricklen, M. et al. (2008). Mobile Device Management. US Patents Patent no. US 20080070495 A1 [Online]. Available from: http://www.google.com/patents/US20080070495 [Accessed: January 17th 2015].

Thielens, J. (2013) Network Security: Why APIs Are Central to a BYOD Strategy. *Network Security*. [Online] 2013 (8).. pp 5-6. Available from - http://www.sciencedirect.com/science/article/pii/S1353485813700916. [Accessed: July 5th 2014.]

Thomson, G. (2012) BYOD: enabling the chaos. *Network Security*. [Online] 2012 (2). pp. 5–8. Available from: http://www.sciencedirect.com/science/article/pii/S1353485812700132. [Accessed: July 5th 2014].

USA. Cisco Systems Inc. (2012) *Bring Your Own Device.*USA. Cisco Public Information.

USA. Sophos Limited. (2012). *BYOD risks and rewards. How to keep employee smartphones, laptops and tablets secure.* USA. Sophos Whitepaper.

## Appendix 1

**Random Sample Questionnaire**

Dear Respondent,

My name is Gerald Mutoro Wangutusi. I am a post graduate student at University of Nairobi conducting a research on "An adoption framework for Bring Your Own Device (BYOD) for organizations: a case study of Madison Insurance Company Kenya Limited" as a partial fulfillment of the requirement for award of Master of Science Degree in Information Systems. I wish to request your participation in this research for approximately ten to fifteen minutes. The information requested is needed purely for academic research purpose and will therefore be treated with utmost confidentiality. I will appreciate your response coming through on or before November 5, 2014. Kindly tick appropriately the options as guided. Thank you in advance.

**Section A: BYOD User Awareness**

1. What is your age category?
    a. Under 25
    b. 26 – 30 years
    c. 31 – 35 years
    d. Over 35

2. What academic qualification do you hold?
    a. Diploma
    b. Graduate
    c. Post graduate
    d. Other (Please specify below)

3. Of the mobile devices listed below, which ones(s) do you own and use at the work place? (Tick all that apply)
    a. Smartphone
    b. Laptop
    c. Tablet
    d. Other (iPod, Kindle, Kobo, MP3 Players)

4. Do you understand security risks of using your device(s) on public Wi-Fi networks?
    a. Yes
    b. No

5. Do you understand what malware is?
    a. Yes
    b. No

6. Do you know what software updates (also known as patches) are? (If "Yes" proceed to 7 else proceed to Section B).
    a. Yes
    b. No

7. Do you install these patches?
    a. Yes
    b. Sometimes
    c. No

8. How often do you install these patches?
    a. When prompted by the computer
    b. I search for available software patches through the Internet and install
    c. Never

**Section B: BYOD User Trends**

1. Do you use your mobile device(s) on other wired or wireless networks (hotspots) such as coffee shops, restaurants, at home?
   a. Yes
   b. No

2. Do you have an anti-virus installed in your mobile device(s)? (If "Yes" proceed to question 3 else go to question 4).
   a. Yes
   b. No

3. Is your anti-virus application up to date?
   a. Yes
   b. No
   c. I don't know

4. Do you store company data (emails correspondences, file attachments etc) on your portable device(s)?
   a. Yes
   b. No

5. Could someone access your data if your Smartphone/laptop/tablet were stolen right now?
   a. Yes
   b. No
   c. I don't know

6. What security measures do you have enforced on your device(s) such as laptops/tablets and/or Smartphone? (Tick all that apply; if "None, go to 12)
   a. PIN codes

b. Passwords
c. Biometrics
d. Pattern codes
e. None

7. If you use password, what comprises of your passwords (else skip to Question 8)?
    a. Plain text of less than seven characters
    b. Plain text of more than seven characters
    c. Plain numerals (less than seven digits)
    d. Plain numerals (more than seven digits)
    e. Combination of text and special characters such as commas, asterisks, harsh etc

8. How often do you change your security measures?
    a. Every 3 months
    b. Every 6 months
    c. Every 9 months
    d. Every year
    e. Never

9. Have you ever shared your device(s) security measures?
    a. Yes
    b. No

10. To approximately how many people?
    a. One person
    b. Two people
    c. Three people
    d. More than three people
11. Did you change this security measure afterwards?
    a. Yes
    b. No

12. Other than requesting MICKs ICT staff for assistance, would you ask a friend who is IT savvy to trouble shoot your device(s)?
    a. Yes
    b. No

**Appendix 2**

**Expert Sample Questionnaire**

If you have trouble viewing or submitting this form, you can fill it out online:
https://docs.google.com/forms/d/1tGWOUqMqe_ZpL8l88LmJltRoQSHlJsTj88qi2Hp8Hzk/viewform?c=0&w=1&usp=mail_form_link

# Questionnaire

Dear Respondent,

My name is Gerald Mutoro Wangutusi. I am a post graduate student at University of Nairobi conducting a research on "An adoption framework for Bring Your Own Device (BYOD) for organizations: a case study of Madison Insurance Company Kenya (MICK) Limited" as a partial fulfillment of the requirement for award of Master of Science Degree in Information Systems. I wish to request your participation in this research for approximately ten to fifteen minutes. The information requested is needed purely for academic research purpose and will therefore be treated with utmost confidentiality. I will appreciate your response coming through on or before November 5th, 2014. Kindly tick appropriately the options as guided. Thank you in advance.

* Required

## Section A: Information Security Threats BYODs Present At MICK

**1. Are you fully aware of all MICKs agents who access company information or applications? ***

- o ( ) Yes
- o ( ) No

**2. Regarding agents using BYODs, what concerns you most? ***

Choose One

- o ( ) Compliance
- o ( ) Downloads
- o ( ) Capacity of IT to support a myriad of devices
- o ( ) Data Security
- o ( ) Loss of Devices

**3. Of the agents BYODs within the MICK network, which of the following activities is of the greatest concern?** *

Choose One

- o ( ) Gaming
- o ( ) Heavy Streaming (e.g. video and multimedia apps like Netflix, Amazon etc)
- o ( ) File Sharing Applications (e.g. download of web content legally/illegally etc)
- o ( ) Non-productive material (e.g. gambling, random web-surfing, chatting, adult entertainment etc)

**4. In your opinion, what threats have agent's BYODs presented at MICK with regard to information security?** *

**5. Which of the following steps, if any, has your IT department taken to protect agent's BYODs?** *

Select all that apply

- o [ ] Running software updates
- o [ ] VPNs
- o [ ] Installed anti-virus software
- o [ ] Restricting/blocking access to certain websites
- o [ ] Network certificates
- o [ ] Restricting access to certain employees
- o [ ] Added a password/PIN
- o [ ] Restricting downloads

**6. How often are MICK agents required to change their passwords/PINs?** *

- o ( ) Monthly
- o ( ) Every 2 - 6 months
- o ( ) Every 7 - 12 months
- o ( ) Less than once annually
- o ( ) Never

**7. How important do you find each of the following BYOD security measures in helping to protect company information? Please answer for each even if your company does not employ the protection? ***

| | Not important at all | Not very important | Somewhat important | Very important |
|---|---|---|---|---|
| Anti-virus programs | ( ) | ( ) | ( ) | ( ) |
| Network certificates | ( ) | ( ) | ( ) | ( ) |
| Software updates | ( ) | ( ) | ( ) | ( ) |
| Access restrictions for certain employees | ( ) | ( ) | ( ) | ( ) |
| Usage Limits | ( ) | ( ) | ( ) | ( ) |
| VPNs | ( ) | ( ) | ( ) | ( ) |
| Mobile Device Management (MDM) applications | ( ) | ( ) | ( ) | ( ) |
| Mobile device encryption | ( ) | ( ) | ( ) | ( ) |

**8. What specifically have you communicated to your employees to protect themselves against cyber-security threats on their mobile devices, if anything?**

Choose two

- o [ ] Importance of running updates
- o [ ] Importance of encrypting messages to protect sensitive information
- o [ ] The need to report data security issues urgently
- o [ ] Importance of changing passwords and PINs regularly

- [ ] Importance of accessing information when on secure networks (e.g. those that require passwords)

**9. Whose primary responsibility is it to keep your employee's personal mobile devices secure when they are accessing company information or applications?**

- ( ) The company's
- ( ) The employees

**10. When employee's access work-related information or applications with their mobile devices, how concerned are you about each of the following? ***

| | Not concerned at all | Not very concerned | Somewhat concerned | Very concerned |
|---|---|---|---|---|
| Employees abusing BYOD | ( ) | ( ) | ( ) | ( ) |
| Security of the devices | ( ) | ( ) | ( ) | ( ) |
| Data protection | ( ) | ( ) | ( ) | ( ) |
| Device could be lost or stolen | ( ) | ( ) | ( ) | ( ) |
| Visibility of all devices that are accessing company informational assets | ( ) | ( ) | ( ) | ( ) |
| Compatibility of devices | ( ) | ( ) | ( ) | ( ) |
| Performance of the device | ( ) | ( ) | ( ) | ( ) |
| Provision of IT support for personal devices | ( ) | ( ) | ( ) | ( ) |

**11. What do you think about BYODs in terms of its benefits against its risks?** *

- o ( ) Risks strongly outweigh benefits
- o ( ) Risks somewhat outweigh benefits
- o ( ) Benefits somewhat outweigh risks
- o ( ) Benefits strongly outweigh risks

## Section B: Vulnerabilities of MICK's ICT Infrastructure With Regard to BYOD

**1. Does MICK have any Mobile Device Management (MDM) application in place to monitor BYOD activities?** *

- o ( ) Yes
- o ( ) No

**2. What actions are taken on a new employee's device when the employee joins MICK?** *

**3. What actions are taken on employee BYODs when the employee leaves MICK?** *

## Section C: MICK's BYOD Policy

**1. Does MICK have a formal BYOD policy? ***

If "No", proceed to 4 then 5 else proceed to 2, 3, 4 and 5

- o ( ) Yes
- o ( ) No

**2. When did MICK put its BYOD policy in place?**

- o ( ) Within the past year
- o ( ) Within the past 1 - 2 years
- o ( ) In the past 3 - 4 years
- o ( ) In the past 5 years or longer

**3. Which of the following does your BYOD policy cover?**

Please select all that apply

- o [ ] Protection for employees related to privacy and loss of personal information
- o [ ] Back-up and restore for personal data if an employee loses or inadvertently wipes their mobile device
- o [ ] Back-up and restore for personal data if their mobile device is hacked
- o [ ] Other: [ ]

**4. Which of the following would you want your BYOD policy cover?**

Please select all that apply

- o [ ] Protection for employees related to privacy and loss of personal information
- o [ ] Back-up and restore for personal data if an employee loses or inadvertently wipes their mobile device
- o [ ] Back-up and restore for personal data if their mobile device is hacked
- o [ ] Other: [ ]

**5. What concern will you want your BYOD policy to address? ***

**6. With/without a policy in place, does MICK provide IT support for its BYODs?**

Please select all that apply

- ( ) Yes
- ( ) No