INFORMATION SECURITY CONCERNS AROUND ENTERPRISE BRING YOUR OWN DEVICE ADOPTION IN SOUTH AFRICAN HIGHER EDUCATION INSTITUTIONS

Submitted in partial fulfilment of

the requirements for the degree of

Master of Science

of

Rhodes University

Gershwin Ashton Sauls

November 2015

Abstract

The research carried out in this thesis is an investigation into the information security concerns around the use of personally-owned mobile devices within South African universities. This concept, which is more commonly known as Bring Your Own Device or BYOD has raised many data loss concerns for organizational IT Departments across various industries worldwide.

Universities as institutions are designed to facilitate research and learning and as such, have a strong culture toward the sharing of information which complicates management of these data loss concerns even further. As such, the objectives of the research were to determine the acceptance levels of BYOD within South African universities in relation to the perceived security risks. Thereafter, an investigation into which security practices, if any, that South African universities are using to minimize the information security concerns was carried out by means of a targeted online questionnaire.

An extensive literature review was first carried out to evaluate the motivation for the research and to assess advantages of using Smartphone and Tablet PC's for work related purposes. Thereafter, to determine security concerns, other surveys and related work was consulted to determine the relevant questions needed by the online questionnaire. The quantity of comprehensive academic studies concerning the security aspects of BYOD within organizations was very limited and because of this reason, the research took on a highly exploratory design. Finally, the research deliberated on the results of the online questionnaire and concluded with a strategy for the implementation of a mobile device security strategy for using personally-owned devices in a work-related environment.

Table of Contents

List of Tables

List of Figures

Acknowledgements

Thanks to James Connan, my supervisor for dedicating his time, his patience, encouragement, ideas, guidance and advice around research design. This project would not have been possible without his support.

Thank you to my family and friends for their constant optimism and belief in me throughout the project; in particular, Charne Phillips for her love and support.

A special thanks also goes to Michael Irwin and Karl Van Der Schyff for sharing their suggestions, ideas and opinions.

Thank you to my Rhodes University work colleagues, who filled in when I was not able to be completely available due to the many hours needed to concentrate on this project.

A final thank you goes to the Rhodes University and the Computer Science Department for providing me with the knowledge to prepare me for and the resources with which to undertake this research. In particular, my thanks go to Barry Irwin, for putting together such an enriching course.

Glossary of Terms

ARM – Advanced RISC Machines, family of low cost, power-efficient microprocessor architectures and peripherals.

API – Application Programming Interface, a set of routines, protocols, and tools for building software applications.

AUP – Acceptable Use Policy, set of rules applied by organizations that govern use of networks, IT services and computer systems.

Botnet – Collection of Internet connected programs, often used to send spam or participate in distributed denial of service attacks.

BYOD – Bring-Your-Own-Device, the practice of employees using personally-owned technology such as smartphones and tablet computers for work related purposes.

Consumerization of IT – The combination of personal and business use of technology devices and applications.

CTO – Certified Technology Officer

Crimeware – Economically motivated malware.

CVE – Common Vulnerabilities and Exposure Identifiers, a system which provides references to publicly known information security vulnerabilities.

Desktop Computer – A computer designed to fit comfortably on top of a desk, typically connected physically to a monitor, keyboard and mouse and various other input and output peripherals.

Dumb Terminal – Display monitor that has no processing capabilities but simply displays output from a mainframe.

HE – Higher Education (Institutions), refers to learning institutions such as universities.

HTML – Hypertext Markup Language, the authoring language used to create documents that contain text, font, colour and graphic effects on the World Wide Web.

ICT – Information and Communications Technologies.

IT - Information Technology

Information Security – Techniques for ensuring that the confidentiality, integrity and availability of data stored in computer systems cannot compromised by individuals without authorization.

Identity Management (IdM) – Method of controlling access to information resources within information systems by associating user rights with associated identities.

LAN – Local Area Network, refers to a computer network which is limited to a single location and smaller geographical area such as an office building or a university.

Lightweight Directory Access Protocol (LDAP) – An open vendor-neutral directory service that contains a set of protocols for accessing distributed information directories.

Malware – collective term for malicious software such as Viruses, Worms and Trojans

Mainframe – A very large and expensive computer capable of supporting hundreds, or even thousands, of users simultaneously.

Minicomputer – A midsized computer. In both size and power, minicomputers fall between workstations and mainframes.

Mobile Device – extremely portable handheld computer with similar features do desktop and laptop computers.

Mobile Device Management (MDM) – A software based suite that allows network enforcement of security policies, configurations and generally allows full control of mobile devices.

Mobile Application Management (MAM) – A software-based security suite that focuses on securing access and actions of applications on mobile devices rather than control the entire device.

Mobile Content Management (MCM) – Security focused mobile management suite that focuses on secure document management through authentication and authorization.

Network Access Control (NAC) – Technique used to monitor and approve which endpoints are allowed to connect to organizational networks.

NIST – The National Institute of Standards and Technology.

OHA – Open Handset Alliance, collaboration of technology companies that include mobile operators, handset and component manufacturers as well as software developers.

PC – Personal Computer; a small, relatively inexpensive computer designed for an individual user.

POPI – Protection of Private Information Act.

SANReN – South African National Research Network.

Security Policy – A document that states in writing the organizational plan to protect the company information assets.

Security Vulnerability – An unintended flaw in software code or a system that leaves it open for exploitation.

Security Threat – an expressed potential to exploit vulnerabilities in a computer system with the intention of doing harm.

Shadow IT – IT solutions built and used within organizations without organizational approval.

Smartphone – handheld device that integrates mobile phone capabilities with the more common features of a handheld computer.

Tablet – A *tablet* is a wireless, portable personal computer with a touch screen interface. The form factor is typically smaller than a notebook computer but larger than a smartphone.

Trojan – derived the Trojan Horse in Greek mythology, it encompasses malware, often disguised as legitimate software, when executed on a target system carries out the malicious code determined by the nature of the trojan.

USA – United States of America

Virus – Malicious software that replicates itself when executed by copying itself into other programs.

WAN – Wide Area Network, similar to a LAN in functionality but is not limited to a single geographic location. WAN's are often composed of several smaller LANs and are interconnected by telephone lines, satellite links and/or fibre optic cables.

Worm – Malicious software that replicates itself to spread to other computers without needing to be executed.

Chapter 1 – Introduction

1.1. Research Area

The concept of "*bring your own device*", shortened into the more popularized acronym "BYOD" is not a contemporary one. The collective term describes the practice of employees using personally-owned technology, for work related purposes, both within their office environments as well as from remote locations. Whilst the blanket term "bring your own device" could potentially encompass the use of personal devices in any field, the hype around the term has stemmed from recent technological advancements specifically in Information and Communications Technologies (ICT). Technologies such as cloud-computing services, web applications, social networking, Internet collaboration tools, wireless networking, mobile broadband networks such as 3G as well as laptops, smartphones and tablet computers have all contributed to the mobile computing opportunities that users have today. Some of these, such as social networks, various web applications, smartphones and tablet computers have originally been designed as consumer only products but the use has shifted, with users wanting to leverage the device usability for work related purposes, creating a contemporary concept known as the "Consumerization of IT" [1]. Although the two concepts are often confused into being the same, the difference is that BYOD refers specifically to the devices which are being used for the purpose described above.

Employees have for a while been using their personal laptops and even desktop computers to access and locally store corporate data, either remotely or with their machines directly connected to the local enterprise network. As such, the concept is not entirely new and has been around for a few years. However, in recent times, there has been a sudden growing interest in the use of user-provisioned technology for business use in organizations. The reasons for this stem from the user realization that there are other computing technologies available that enable them to perform similar work-related functions with the contemporary devices they personally own versus the devices which have traditionally been provisioned by their institutional Information Technology (IT) Department. Smartphones and tablet computers have played a big role in this realization, as the user experience offered with these, gives users similar ease of use and adaptability that have long been only available on the traditional desktop Personal Computer (PC). The combination of maturing mobile operating systems and device portability has exaggerated this personal preference even further. This study therefore focuses specifically on these mobile technologies and the security concerns effected by the devices that are relevant to IT Consumerization.

Smartphones and tablet devices have advanced in recent years with an ever increasing amount of data storage and computational processing power. The recent popularity of consumer devices is also heavily related to wireless networking advancements and a global increase in Internet bandwidth availability. This influential combination has had a positive impact and escalation in end-user productivity and mobile computing capabilities on such devices. A jointly-funded 2012 study between Dell and Intel which included more than 8,000 workers and 29 global executives confirms this. *"Workforce productivity has increased by allowing employees choice in their computing devices. Expanding work privileges to allow for more mobile workers also boosts overall productivity. And, shockingly straightforward, the survey reveals that employees who work on the devices they love in places they prefer quickly, optimize their outputs"* [2]. The small form factor and portability of these devices augments their mobile computing possibilities and makes it obvious how, as well as why, business users would want to carry this functionality over into the workplace.

For consumers, these personal mobile devices have become an indispensable communication tool throughout their day-to-day lives and workers now want to carry this over to their office environments. This brings new security implications for corporate networks, as mobile devices, due to their improved capabilities are now susceptible to vulnerabilities and malicious applications in a similar manner that traditional desktop computers are. In the corporate world BYOD is the idea of employees using their personal desktops, laptops, smartphones, tablet computers or any other Internet-capable device to access corporate data for work related purposes. In the context of educational institutions such as universities, the use of personal mobile devices for work extends beyond employees to research associates, visiting lecturers, students, vendors and various other similar entities. For educational institutions, these devices offer both staff and students learning opportunities and continuous access to educational resources. As such, smartphones and tablet PC usage offers both administrative, as well as learning opportunities in higher education institutions.

1.2. Motivation

These easily recognizable advantages offered to consumers and organizations through mobile computing however introduces various hidden disadvantages such as the risk of information loss to the institutions that allow their use. Cyber-criminals now have additional avenues for attack and are aware of these. Within the scope of Information Security practices, attack vectors such as these are referred to as vulnerabilities. If not addressed, there exists the possibility that these will be exploited to leverage further attacks as has been done with desktop and laptop computing endpoints, which have traditionally been used as one of the primary initial attack vectors. Mobile computing has effectively broadened the traditional endpoint perimeter so it is essential that institutions carefully implement the relevant security practices. In so doing, a large portion of such threats will successfully be minimized.

For most organizations, the risks associated with information loss is usually an afterthought or the efforts concerned with protecting that information is seen as a hindrance to productivity. Educational institutions such as universities have a culture of information sharing which hereby exacerbates this belief even more. All too often, only once a data breach occurs and the true risk is realized, do organizations think about implementing mitigating strategies to protect against cyber-crime and information loss.

Higher education institutions have a wealth of sensitive information that should be protected. Some examples of these are, intellectual property, sensitive research, academic records, financial records, salary records as well as employee staff and student private information records [3]. Cyber-criminals use information gathering techniques before carrying out attacks and therefore often seek any information that they are able to harvest with the intention of using the gathered information to augment further attacks. As an example, social engineering attacks have evolved into sophisticated context aware phishing attacks, also known as *spear-phishing*, where the attacker uses specific knowledge of the individuals and their organizations to gain trust and increase the likelihood of success [4]. Cyber-criminals are looking to harvest any information that may ultimately lead to resources that have financial value attached to them.

1.3. Problem Statement

User provisioned mobile devices such as smartphone and tablet PC's provide numerous productivity and educational benefits to universities. Conversely these devices also introduce new threats to privacy and loss of sensitive information. To demonstrate by example and comparison to more familiar endpoints such as desktop workstations, mobile devices are much smaller and therefore easily lost or stolen, taking corporate data out of the business controlled environment and into the public domain. To further compound the issue, the sheer volumes of different hardware and software models, together with exponentially increasing amounts of feature enhancements and software applications for the devices, add even more confusion and complexity for internal IT Support Departments because of the lack of organizational device control.

Mobile malware attacks, unauthorized access to company internal networks, even mobile botnets have now started to emerge as threats on smartphone and tablet computers. This now creates an immediate need for organizational mobile device security policies to manage these risks [5]. For Universities, this problem is even more complex because the institutions by nature have a culture of information sharing, which makes such policies even harder to construct to achieve the balance between usability and security. Within the information systems of any organization, these issues fall strongly under the domain of Information Security, which is the focus of this research.

1.4. Objectives of Research

This study is an exploration into the information security strategies, if any, that higher education institutions in South Africa have put in place to address the threats introduced as a result of the Bring-Your-Own-Device phenomenon and as such the primary objective of this research is to investigate the acceptance and security maturity levels of ICT Divisions within higher education institutions in relation to BYOD to assess the readiness of South African institutions to defend against the associated threats. The secondary objective is to examine the aspects necessary for the implementation of a secure mobile device adoption strategy while still maintaining the usability and mobility advantages of personally-owned mobile devices. This moves the study from an investigative phase of the current defense strategies of respective institutions against potential information loss from BYOD, toward practical advice in the form of changes to organizational security strategies based on the issues identified during the investigative phase.

The primary goal is to contribute to academic literature with regards to the information security concerns around enterprise BYOD adoption and hereby provide insight for further research. The secondary goal of the dissertation is to provide some insight and guidance for university Network System Administrators, Information Security staff and ICT Director's for security considerations when implementing a BYOD strategy within their respective institutions. This guidance could also be used by other institutions outside the scope of higher education that need to find a similar balance between the productivity advantages of BYOD and the information security risks.

1.5. Research Questions

In light of the above objectives, the study intends to answer the following research question:

> Are South African universities adopting BYOD and are they aware of the information security concerns introduced into their organizations by allowing this practice? If so, which strategies if any, are being used to minimize these concerns?

Taking this primary research question into account, the following sub-questions are developed and used to guide the researcher during the research process and assist in achieving the aforementioned objectives:

1. Do universities have sensitive data that is worth protecting? What security risks are universities faced with and do personally-owned mobile devices increase this risk?

2. What is BYOD? Define the concept and explore the sudden interest of employee's using personal mobile devices for work related purposes.

3. What are the current acceptance levels of BYOD within organizations and does this compare to the acceptance levels within South African higher education institutions?

4. What security threats to organizational data are introduced by these personally-owned mobile devices?

5. What does the related research inform us about organizational mobile device adoption in relation to BYOD and which strategies are organizations using to mitigate any associated threats?

1.6. Study Methodology Overview

The study will be conducted in three phases:

1. A review of relevant literature
2. A targeted online questionnaire
3. Best practice recommendations

The literature survey process involves careful review and content analysis of other similar studies for recurring themes related to organizational information security practices around personally-owned mobile devices. Many of the surveys related to mobile device security implications for organizations are conducted by industry analysts, as at the time of this writing, academic literature around the subject is sparse or only addresses specific mobile technologies and not strategies to minimize security risks in organizational settings that are related to these risks. The existing literature is analyzed with the aforementioned sub-questions in mind to determine the necessary survey objectives for the online questionnaire.

The review of literature also serves to form background knowledge to define the concept of BYOD and to recognize why it is significant enough for Information Security practitioners to devote attention to the sudden occurrence of personally-owned mobile computing devices in work related environments. This then forms a basis of the discussion.

A targeted online questionnaire is thereafter sent to individuals who have previously been identified as having senior technical positions within IT Divisions of participating South African universities. The aim of the questionnaire is to investigate the unanswered questions which are discovered through the available literature. The questionnaire therefore serves three purposes, (1) to determine the adoption level of BYOD in South African universities; (2) to determine the opinions of technical staff around the various issues from a security perspective that are presented by using personally-owned mobile devices in their respective institutions; and (3) to determine the strategies, if any that are being used by South African universities to mitigate BYOD related threats.

Finally, this thesis provides the reader with best practice approaches for the mitigation of security related threats introduced by mobile devices with recommendations for changes to institutional security strategies. Due to the recency of the subject, much of the literature around policies, best practice models or control recommendations come from a combination of academic literature as well as industry studies and a synthesis of these will be used to advise on the recommendations.

1.7. Research Context

Due to their recent popularity which has led to the push toward BYOD working environments, the research discussion focuses on current mobile platforms relative to smartphones and tablets only. Findings from the literature review seek to determine which of these device platforms are current. Whilst any controls for securing the information associated with these devices should focus on encompassing all of the device types, the recommendations given are not limited specific to any smartphone or tablet platforms. The nature of the BYOD trend in itself is not bound to any specific technology, but rather lets users decide which devices they prefer to use. As such, any recommendations rather place an emphasis on the information security related processes and not specific technologies. Throughout this research, laptops and other similar conventional “mobile” Internet-connected devices will also be discussed but these will not be debated at length as the focus is on the devices that have brought about the recent trend in use of personally-owned devices within organizational settings. In the context of this research, when referring to ‘mobile devices’, the study is predominantly referring to Internet-connected hand-held computing devices which have integrated cell-phone technology.

1.8. Research Limitations

This study is limited to higher education institutions in South Africa that fall under the category of “University”. These include traditional universities, comprehensive universities as well as universities of technology, formerly known as Technikons. It may be assumed that whenever the term ‘*Higher Education*’ is used within this study, the reference is limited to universities and excludes other types of tertiary education institutions that may also fall under the umbrella of higher education. There are to date, a total of twenty-three universities in South Africa.

A further limitation is that each participating institutions primary education model, needs to have a physical campus where students attend lectures and have high-speed Internet access from a physical network infrastructure within a localized area. It is presumed that all major South African universities have some form of Internet access from within a Local Area Network (LAN). This presumption is based on the 2007 implementation by the Council for Scientific and Industrial Research (CSIR) of the South African National Research Network (SANReN). SANReN is a high-speed network which has been dedicated to research and education which is part of the South African governments approach to enable South African researchers to participate with the global research community [6]. The network which is operated by the Tertiary Education and Research Network of South Africa (TENET) in collaboration with the CSIR, includes a 10 Gbps backbone as well as fibre rings in Johannesburg, Pretoria, Cape Town and Durban [7].

Considering the above criteria, the University of South Africa (UNISA) which is the only exception to this model and is hereby excluded from the study due to the nature of their physical network infrastructure being vastly different from the other twenty-two institutions. This is because although small physical campuses exist within the institution, UNISA operates primarily under an open distance learning education model and therefore the majority of their learners are not in attendance of lectures and do not directly connect their devices to campus networks.

This study aims to explore the information security practices that South African universities have implemented with regards to BYOD at the organizational level and as such, the target group for the questionnaire are university staff members holding senior positions within their respective IT departments. For this reason, only a single representative with either managerial or senior technical experience from each of the twenty-two South African universities is deemed necessary.

1.9. Document Layout

This document is further arranged into 8 chapters as detailed below:

Chapter Two – Background

This chapter begins the literature review and discusses the security concerns that affect universities. Examples of the various types of sensitive information stored by universities are discussed and examples of actual cyber-attacks against universities are given to demonstrate the threat impact. The history of various endpoint computing devices and the evolution toward mobile computing is discussed to provide an understanding of the advantages introduced by the convergence of mobile and desktop operating systems in the workplace are presented to the reader. Evidence of the current practices, acceptance levels in organizations and BYOD adoption in universities. This provides the reader with an insight into the advantages and usage possibilities that BYOD provides to organizations.

Chapter Three – Technical Discussion

This chapter provides an analysis of the increasing threat of mobile device targeted malware. An analysis of mobile threats, vulnerabilities and exploitation trends that are associated with past and current mobile devices are also presented to form an understanding of the disadvantages for organizations by allowing the use of personally-owned mobile devices for business use within organizations.

Chapter Four – Related Research

This chapter provides analysis of the works of other researchers which is most closely related to the topic of security concerns surrounding mobile device use within universities as well as other organizations.

Chapter Five – Research Design

This chapter discusses the research design, the relevant tools used during the study and the reason for the methodology choices.

Chapter Six – Questionnaire Results

This chapter discusses the results obtained in the questionnaire and compares these with key points learned from literature.

Chapter Seven – Recommendations

This chapter provides guidelines and strategies for implementation of secure strategy for BYOD adoption.

Chapter Eight – Conclusion and Future Work

This chapter concludes the study and provides a discussion of future work.

Chapter 2 – Background

Before considering the security risks that mobile devices introduce into South African universities, it is necessary to form an understanding of the general information security concerns that universities are faced with. The following chapter provides a discussion on these concerns and thereafter, provides a background of the evolution of endpoint computing, from traditional desktop computing toward mobile computing. This background is needed in order to understand why mobile device use within organizations have become so pervasive for work-related computing purposes. Lastly, device adoption, current practices and some examples of practical use of mobile devices within other organizations and in universities are provided.

2.1. Information Security Concerns for Universities

Kerievsky [8] realized the need for the protection of university information resources in computer and network environments as far back as 1976. University networking infrastructures have been designed to accommodate staff, students, visitors and researchers with the capability to share large amounts of data between them. As a result, university networks have been a target first because the huge amounts of computing power they hold; and second because of their open, often exposed access they provide to their users and in some cases even the public [9].

Before evaluating the vulnerabilities and threats which mobile devices introduce into organizations, it is necessary to point out why institutions such as universities would need to be concerned about protecting their information assets.

2.1.1. Sensitive Information stored by Universities

Universities store large volumes of sensitive staff and student information such as financial records, academic records and personally identifiable information which could be misused by both external threats such as cyber-criminals, as well as internal threats such as disgruntled employees and students. This could result in the institutions facing reputational damage as well as financial losses. Vacca [10] states, "before risk can be measured, the organization must identify the vulnerabilities and threats against its mission-critical systems in terms of business continuity”. The author further states that risk is “determined as a product of threat, vulnerability and asset values” and herewith develops the equation:

$$Risk = Asset \times Threat \times Vulnerability$$

While threats and vulnerabilities are equally significant components of risk analysis, before any organization is able to assess the information security risks, it is necessary to first identify and classify the information assets which are deemed critical or contain sensitive or confidential information which the organization cannot afford disclosure of. Digital data, may be categorized in terms of the need for protection into categories such as public, internal, sensitive and restricted classes.

2.1.2. Examples and characteristics of data classification in Universities

Public Information

This is the least sensitive category and includes information such as course catalogues, syllabus and research data sets which have had their identification information removed. If such information were released into the public domain, the institution would not be negatively affected in any way.

Internal Information

This would encompass any information that should preferably remain confidential to the institution but may be more open to disclosure to facilitate information sharing. Some examples of these are budget plans and email correspondence regarding general internal matters. For an attacker, this kind of information may be used for exploratory or investigative purposes to augment access to more sensitive information. For this reason, universities would prefer to restrict access to this information only to necessary parties whenever possible.

Sensitive Information

Any information which needs to be protected for operational, ethical, proprietary or privacy reasons should be categorized as sensitive. There may be no legal requirements to safeguard the information within this category but it is within the institutions best interests to maintain the confidentiality and integrity of such data. Examples of these are, research information which include identifiable human subjects, salary records, alumni records, student academic records, as well as internal investigative records. Infrastructure and operational specific data such as ICT systems and network plans also fall under the sensitive category and may provide a gateway to additional restricted data. For this reason, sensitive data should be treated with strict levels of access control.

Restricted Data

The loss of integrity, confidentiality or availability of any information which may have a significant negative effect on the institution financially or its reputation, should be regarded as restricted. The protection of the information that fall under this category may also be mandatory due to government legislation such as the Protection of Personal Information Act (POPI) which was signed into law in November 2013[1] by the South African government. POPI places restrictions on how companies handle private user data, defined as personally identifiable information by the Electronic Communications Act (ECT) of 2002. Examples of such restricted data in universities include employee personal information, student personal information such as their national identification numbers (SA ID Number), patient health information, financial records and credit card information. Authentication information such as usernames and passwords should also be considered restricted as these may allow access to other restricted information if not adequately protected.

This knowledge of the various examples of sensitive information stored by universities comes from the personal experience of working in a South African university for a number of years. Once the data has been classified and inventoried, in this way, the controls that need to be implemented

[1] http://www.justice.gov.za/legislation/acts/2013-004.pdf

for secure mobile device access become easier to establish. University business activities are diverse in nature because of the various research and teaching practices that are used by individual institutions and because of this, these data classification categories and their contents would need to be assessed on an individual basis by each institution.

2.1.3. Information Security Attacks against Universities

In order to for any organization to understand the risks which may affect the confidentiality, integrity and availability of their information assets, it is worthwhile also exploring the impact. Impact further demonstrates asset value and for this reason the following section presents recent examples of security incidents which negatively affected universities and the resulting impact for the institutions.

In February 2014, the University of Maryland (UMD) in the United States of America (USA) experienced a computer security attack that exposed personal information records of faculty staff, students and affiliated personnel [11]. Reports suggest that the breached database allowed the theft of 287,580 such records, dating back to 1998 as well as student only records who attended the institution between 1992 and 1998. The cause of the breach was still under investigation by computer forensics teams and federal law enforcement authorities at the time of writing and as a form of compensation, UMD offered free credit-protection services with a third-party company for five years for all those affected. While the institution has not made available the total sum of the costs of the breach, cyber security insurance experts estimated the figure to run into millions of US dollars [12].

In March 2014 an incident at the University of California San Francisco which involved the physical theft of desktop computers at the institution resulted in the university medical center notifying 10,000 patients about a breach of their personal and healthcare information. This was the third reported computer theft incident at UCSF within a period of six months and the stolen machines contained information such as patient names, dates of birth, mailing addresses, medical record and health insurance ID numbers, as well as driver license numbers. Again, in this case the solution was to offer the affected individuals credit monitoring services. For criminals, such information is of value for the purposes of identity theft and causes unnecessary costs for the affected institutions. Additionally, it is worth highlighting that this incident was caused by the theft of physical desktop machines. Recent computing technologies favour smaller devices such as laptops, tablet computers and smartphones and thus increase the likelihood of theft even further.

In May 2014, a data breach at Butler University in Indianapolis leaked personal information of staff, students and alumni [13]. Third-party forensics expert analysis revealed the extent of the breach affected approximately 163,000 individuals and that the compromised data included names, dates of birth, Social Security numbers and bank account information. The individuals affected by the breach were offered one year of free credit monitoring services. What was alarming about this data breach was the institution only learned about the data breach when law enforcement officials who were conducting an identity theft investigation discovered a flash drive on one of the suspects that contained personal information of Butler staff members. Only then was an external forensics team appointed to discover that the university's network had already been breached in November 2013 and was therefore exposed for months until discovery from external sources. This demonstrates that the institution may have been in the undiscovered state indefinitely for an even longer period if not for coincidental investigations by law enforcement.

Incidents of data breaches in South African higher education instittions are not widely reported and offer minimal detail for the existing reported incidents. The reasons for this are unclear and could indicate that the institutions are exceptionally secure or that cyber criminals see little value in attacking in South African universities yet. It is also likely that the institutions do not publicly report incidents to minimize reputational damage or are unaware of the extent of security breaches in a similar way that Butler University was until made aware of the breach by an external investigation.

2.1.4. Summary

Universities accumulate a large amount of both personal and financial data and it is thus unsurprising that cyber criminals have directed their efforts at these institutions. Leakage of such protected information could be used for various criminal activities such as identity theft, intellectual property theft and financial fraud, thus involving the institutions in unnecessary expensive litigation if adequate measures of protection have not been implemented.

There are demands for universities to “cater for emerging patterns on educational involvement which facilitate lifelong learning and to include technology-based practices in the curriculum [14]”. This serves the purpose of not only keeping the institution abreast with current and new teaching methods but also facilitates learners and researchers with improved methods of obtaining and analyzing gathered information. As such, to provide academic institutions with the ability to make use of newer empowering technologies such as smartphones and tablet PC’s can be highly advantageous to both university staff as well as students when looked at from either personal productivity or teaching and learning perspectives.

What is often overlooked with the adoption of new technologies is that they provide additional attack vectors for information security incidents [15] which may lead to serious financial losses or reputational damage. This inherent information security risk is oftentimes the by-product each time new information technology systems are introduced to the institution.

2.2. Towards a Mobile Computing Enterprise

“*Over the past decade, organizations have sought to become more efficient and productive by adopting information and communication technologies.”*

The above quote from a statement made by Wallace and Baker [15] highlights the important role that Information and Computing Technologies play within organizations today. These technologies have allowed organizations to become more productive and have improved the way businesses communicate and collaborate with each other as well as their employees. As such information systems are seen as critical to the success of large organizations which provide them the ability to freely communicate and process information amongst employees, stakeholders, third-party vendors and partners, both locally as well as globally. As these systems have evolved and improved over time, so too have the ways in which organizations have adopted them for business use.

Berndtsson *et al.* [16] recommend that in order to convince readers that is worthwhile to pursue any project aim, it is necessary to first outline the reasons for the chosen subject. Following these guidelines, the following chapter explores historically how computing technologies have evolved into critical systems for business use and this is then later contrasted to draw similarities for the reasons of adoption of mobile devices for work related purposes today. The background of how this evolution has taken place also demonstrates how various security controls have developed as necessary to accommodate the advancing nature of computing technologies and the associated vulnerabilities.

These computing advancements extend into current mobile devices such as smartphones and tablet computers and a historical analysis of these are also presented to provide an understanding of the benefits versus the risks of using mobile devices for work related purposes. Understanding the user interest of mobile device use for tasks previously limited to traditional computing devices only, is essential in order present a case for the reasoning behind this study.

2.2.1. Endpoint Security Evolution

Between 1940 and 1960, the first generation of computers came about, this was the age of Mainframe computers which were completely stand-alone units that would usually fill an entire room. Only one privileged user was allowed to operate the Mainframe and other users would submit their jobs by means of what was then termed “batch processing” to this operator, who then returned the results for each user. Security was largely centered around maintaining the physical protection of the information that would be processed on that machine itself. The only networking of information in this era was done by human messengers who would physically carry the data to be processed via storage media from one mainframe to the next. As such, the possibility of security breaches was limited to the data being physically lost, damaged or stolen while in transit [17].

The next big step in computing was the Dumb Terminal, which appeared between the late 1960’s until the early 1970’s and allowed multiple users to access and use data which was held remotely on a central mainframe type computer. Dumb Terminals were so named because the terminals themselves did not do any actual processing of the data as this was done centrally on the Mainframe. Securing this remote information distributed between terminals and the central data now moved beyond just simple physical security and user authentication was introduced. Password cracking and sharing of user passwords were problematic as security policies were practically non-existent at the time [17]. Information security practices were still in their infancy as were the technologies that were being used then.

Following Dumb Terminals, Minicomputers and Timesharing computers emerged within business use. Minicomputers were similar to Mainframes only much smaller and instead of taking up an entire room these varied in size but were roughly the size of today's average refrigerator. The reason for the name 'Minicomputer' was that the machines were mini in size compared to Mainframes but not at all mini by 21st century Personal Computer standards. Timesharing computers were the first truly multi-user systems which helped pioneer email, file sharing and many of the features of future networking which allowed for such communication over traditional telephone lines [18]. Along with these new networking capabilities, came new information security concerns like maintaining the integrity of information, which in turn introduced advanced security controls such as access control, digital signatures and public key cryptography[17].

The 1980s saw the introduction of the Personal Computer (PC) which made it possible for both personal users as well as businesses users to each have their own computer [19]. Significantly smaller in size than Minicomputers, the PC allowed users the ability to do all their computer processing on their personal machines themselves which enabled instantaneous response as opposed to the technologies that had come before it. New security threats evolved as a result and the 1980s saw the emergence of computer viruses and worms. The Elk Cloner virus, first reported in 1981 and one of the first reported cases of a computer virus, spread via Apple II PC floppy disks which merely presented the PC user with an on screen poem [17], creating more of an annoyance for the user than being anything malicious.

Within this same decade Local Area Networks and Microsoft Windows started becoming ubiquitous and the Internet, which started out as a closed and trusted research network community originally known as the ARPANET [20], started growing rapidly. PC's allowed users to share information along local wired networks which were rapidly expanding throughout organizations.

In 1988, a researcher named Robert Morris created what is known to the Information Security community as the first noteworthy worm [21]. Aptly named the Morris worm, after its creator, it exploited a zero-day vulnerability to facilitate its propagation over the network. Worms were classified as being different to computer viruses in that they exhibit network self-propagation characteristics and therefore did not require disk to disk replication. Although the Morris worm was not designed with any malicious intent and therefore had no actual malicious characteristics, its discovery was a defining moment for researchers and organizations. This evoked the realization that the Internet was no longer just a closed safe community [20]. In that same year, various companies started developing anti-virus software and one of the first known of such software products was called Dr. Solomon's Anti-Virus Toolkit [17].

Shortly thereafter, in the 1990s, Local Area Networks (LAN) expanded into Wide Area Networks (WAN) and later into the Internet as we know it today. With the growth of the Internet, so too, the hacking community started growing and viruses, worms and malicious code were by now becoming a growing concern for the PC due to easily obtainable hacking software toolkits. Internet crime started becoming more and more prominent and in an attempt to counter this threat, more and more software vendors started releasing anti-virus software. According to Dlamini *et al.* [17], by the end of 1990 there were nineteen such products available on the market.

As computing technologies advanced, so too did the techniques of malware proliferation and by the late 1990s, malware was being distributed via email and web browsers. Cyber-crime was continuously advancing and other attack methods such as distributed denial of service (DDoS) started to appear on the security radar [17]. As a countermeasure for this, commercial firewall products and perimeter security were implemented to keep outsiders out of organizational networks. The first instance of a commercial firewall product was actually available as early as 1991 [20] but it was during the late 1990s that organizations started realizing the need for these due to the varying approaches of attack.

The start of the 21st century saw a major shift in cyber-crime culture. Motives started evolving from amateur script kiddies and hackers seeking to demonstrate their technical abilities to peers, to highly organized professional attacks for financial gain. Throughout the first decade of the 21st century, many technical advances were made from the era of the Personal Computer and ICT infrastructure was becoming highly pervasive across most major industries worldwide [17]. This high adoption and technology advancement soon started developing into a reliance on Information

Systems for all businesses on a global scale. Along with these technological advancements for the PC, various security threats have historically developed alongside which suggests that PC's were not initially designed with inherent security in mind but rather with functionality and usability as a priority. The era of the Personal Computer, which was originally based on the tethered desktop computer model, evolved into various wireless end-user computing technologies such as Laptops, Personal Digital Assistants (PDA) and eventually into mobile devices more popularly known as Smartphones and Tablet computers today.

A significant common characteristic in these contemporary personal computing technologies is the capability of device portability. Not being fixed to a work desk allowed users the ability of reading and processing information at any time of the day from almost any location on condition that the devices in use support this functionality. Wireless networks enhanced this portability even further by allowing users access to information from remote locations essentially over the air. In the well cited guide to 802.11 Wireless Networks [22], the author states *"Users move, but data is usually stored centrally, enabling users to access data while they are in motion can lead to large productivity gains."*

This advantage of mobility adds another layer of complexity for Information Security professionals that needs to be addressed. With computing and information sharing technologies constantly evolving, so too are the security implications that need constant assessment in order to stay abreast of the threats to the often overlooked but precious commodity of information.

2.2.2. Evolution of Mobile Computing

A basic trend that is evident throughout the evolution of computing is that devices themselves are getting smaller and this, along with a combination of various advancements in supporting technologies such as wireless networking and cloud computing has allowed modern computing devices the additional benefit of portability. These advantages already started becoming apparent with the Laptop computer, so the concept of mobile computing is not new. As previously discussed, this advantage also presents physical device vulnerabilities.

The portability of smartphones and tablets have however not been the only reason for their associated vulnerabilities. A brief background of mobile device evolution is necessary to understand these contemporary devices and the threats associated with them. Also it is necessary to determine the need for security efforts to mitigate these threats by analysis of past and present usage trends of personally-owned mobile devices. Mobile computing differs slightly from traditional desktop computing and it is necessary to understand these subtle differences in order to understand the reasons for their significant adoption in organizations.

The differences and evolution between the various mobile device platforms are explored in chronological order in the following section to determine their relevance to this study.

2.2.2.1. Late 1990's

The first instance of a mobile device which had many of the characteristics of the devices known as smartphones today was released by IBM in 1994 and was named the IBM Simon Personal Communicator. Although much bulkier in size at 8 inches in length and 1.5 inches thick, Simon had many of the innovations that are found in modern touchscreen phones [23]. The device had a monochrome touchscreen with on-screen icons and applications such as a calculator, calendar, clock and even a fax machine built into the design. The term Smartphone was not coined yet although the device was the first commercially available product that introduced the ideas of a mobile phone which included similar functionality. Sales of the device ended in early 1995 [23] with several factors acting against its success, the most notable being extrinsic to the device itself in that fast cellular data and wireless networks were not widely available yet. Cellular networks at the time were designed for voice and not data and as a result, the devices were not easily able to retrieve or share information.

The late 1990's saw a steady rise in popularity of mobile computing with the introduction of the Palm line of handheld computers with millions of units being sold worldwide. The proprietary Palm OS [24] operating system allowed for third-party software installation of numerous software applications from various web repositories as well from Compact Disc collections. The major difference between Palm devices and current smartphones were that Palm initially designed handheld computing devices that did not have any phone-like functionality.

2.2.2.2. Early to Mid-2000’s

Advancements in Internet wireless connectivity with networks such as WiFi 802.11 and third-generation (3G) mobile networks had a major influence on how mobile devices would evolve into powerful on-the-go computing devices. The latter, 3G, which today offers mobile devices almost ubiquitous continuous Internet access from any physical location [25], was first commercially available in the early 2000’s with initial data transfer speeds of between 384kbs and 2Mbps. 3G network data speeds enabled voice, video and a rich hypertext markup language (HTML) web browsing experience for mobile phones which then led the direction in which cellular handset manufacturers would design both the hardware as well as software for future devices.

Symbian

The early 2000’s in terms of mobile operating systems, were dominated by Palm OS, Symbian and Microsoft Windows CE Mobile, all of which are currently discontinued. Symbian OS was by far the dominant platform of the three and its parent company of the same name partnered with major cellular phone manufacturers such as Nokia, Ericsson and Motorola to develop mobile devices with a similar feature set commonplace in modern smartphone technology. Symbian however, was not designed for touchscreen devices which sets the platform apart from current smartphones. During this time, mobile devices with only voice calling and text messaging functionality, also referred to today as ‘feature phones’ were still common but the popularity of mobile devices with computing capabilities was persistently increasing.

Symbian provided free publicly available Software Development Kit’s (SDK) along with documentation and emulators for developers and handset manufacturers to create third-party applications which were written in the C++ programing language [26]. The operating system allowed for such applications to be installed via USB synchronization with a PC, directly over-the-air, from the Internet and also via Bluetooth which only allowed wireless connectivity of up to 10 meters [27]. Wi-Fi and 3G network technologies were still in the infancy phase and Bluetooth at the time, was the more popular method of wireless connectivity for mobile devices.

The ability to install third-party applications dramatically increased Symbian usability and popularity amongst device manufacturers and consumers. According to market research reports in

2004, the platform’s market share rose to 53 from 38 percent of overall smartphone market share from the year before [28] with Nokia being Symbian’s major handset contributor. In 2008 Babin [27] wrote that the total number of Symbian smartphones in circulation had surpassed 145 million, with a smartphone market share of 72.4 percent in 2007. At that time smartphones accounted for only 9 percent of the total mobile handset market but this percentage was rapidly growing.

Many online reports confirm that Symbian was leading the market in smartphone sales around this time, but this popularity diminished towards the end of the 2000’s due to competition from numerous other smartphone devices. By the third quarter of 2010, Symbian market share had dropped to 36 percent. Nokia officially announced in 2011 that as a handset manufacturer, they would be partnering with Microsoft instead, replacing Symbian with Windows Phone as their primary smartphone strategy [29]. This confirmed signs of the platform losing popularity and as of this writing, Symbian is currently in a discontinued state.

2.2.2.3. Between 2006 – 2011

In the mid to late 2000’s the availability of faster Internet services through Wi-Fi and cellular data networks continued its growth and allowed mobile device manufacturers as well as software development companies to take advantage of these developments to create an improved mobile user experience. As a result of this, smartphones and tablet computers started becoming a viable alternative to traditional desktop and laptop computers due to major improvements in both device hardware and software functionality.

RIM BlackBerry

Research in Motion’s (RIM) was one of the earlier contributors to this realization of using mobile devices for work related activities. The first BlackBerry device was introduced in 1999 with email and limited web browsing functionality but it was not until the mid to late 2000’s that the platform achieved a sharp increase in popularity. RIM’s initial focus for the BlackBerry platform was on business markets with features such as push email, Microsoft Exchange, Novell Groupwise and BlackBerry Enterprise Server (BES) support [30] being significantly useful for organizations.

BlackBerry Enterprise server offered IT System Administrators, remote management and control for company owned BlackBerry user devices. Policy management features that allowed IT Administrators to remotely wipe all data from lost devices or remotely push [30] software configurations to devices enabled management functionality with BlackBerry's for organizations. The ability to manage user mobile devices with remote policy and remote device configuration proved a strong selling point for the manufacturer. As a result, both business as well as consumer markets thrived and in 2009 the company CEO announced that "…RIM experienced an extraordinary year in fiscal 2009, shipping our 50 millionth BlackBerry smartphone" [31].

Similar to Symbian, BlackBerry made available a Software Development Kit and related documentation for application development with Java. Application distribution was made available via the official BlackBerry online repository, App World, directly from 3rd party software vendors via the device web browser as well as through PC synchronization software [26].

It is important to note that although BlackBerry devices are still available, the device market share has significantly dropped due to competition from Apple's iOS, Google's Android and Microsoft's Windows Phone smartphone and tablet devices. In the fourth quarter of 2009 BlackBerry reported sales of 10,7 million units and by comparison, four years later in the fourth quarter of 2013 sales had dropped to 1.7 million units [32].

Apple iOS

In 2007, technology giant Apple entered the mobile device space and launched the original iPhone running their proprietary operating system iOS [33] which is used exclusively on their, iPod, iPhone smartphone and iPad tablet devices. Some technology experts claim that it was Apple's first iPhone device which realized the usefulness of smartphone devices with the capabilities that rival more traditional personal computing devices such as the PC [34].

What the iPhone did differently to other smartphones was to introduce a multi-touch[2] touchscreen interface, which allowed input directly on the screen instead of via a stylus or a dedicated hardware keyboard. This enabled the phone interface to have a software keyboard, recognize touch gestures and advanced functionality such as pinch-to-zoom and gave the device a fluid, intuitive user interface. The original iPhone had a built-in HTML email client [33], feature rich web browser based on Apple's OSX desktop operating system browser Safari, and very importantly, a user friendly application repository which essentially allowed users to extend the functionality of their device. Later versions of iOS enhanced functionality further and allowed users the ability to quickly switch between active applications, while the operating system would pause inactive applications in memory, thus giving the operating system a feel of multitasking, a feature common in modern desktop operating systems. iOS borrowed many features from its predecessors and catapulted the iPhone into a device with functionality in a handheld device that strongly rivalled traditional operating system functionality.

Apple also provided application developers with documentation, tools and the necessary Application Programming Interfaces (API) to develop applications in the Objective C programming language. These applications would then be made available for download from Apple's official software repository [26] and in so doing, generates revenue from sales for both the third-party developer as well as Apple each time an application is purchased. Unlike other mobile operating systems, all iOS applications are installed exclusively through Apple's own '*App Store'* provided the device has Internet access, either over Wi-Fi or over the device carrier's cellular data network, thus ensuring a constant revenue stream for Apple. Instead of over-the-air, users can also install applications from the App Store using desktop synchronization software iTunes, connected via USB. With either of these installation methods, all iOS applications are installed from the same single repository. Users are not allowed to install applications via any other method with the exception of jailbroken[3] devices, which effectively extend the capabilities of the

[2] "In mobile computing, multi-touch refers to the capability of a touchscreen (or a touchpad) to recognize two or more points of contact on the surface concurrently" http://www.gsmarena.com/glossary.php3?term=multitouch

[3] A form of privilege escalation which allows the user full root access to the iOS file system.

device to operate beyond the default constraints which Apple has put in place, such as installation of applications from unofficial repositories.

In 2006, the three current dominant mobile operating systems, iOS, Android and Windows Phone OS were not commercially available yet, when technology market research firm Canalys reported that sixty-four million smartphones were shipped globally in that year [35]. When the statistics are compared merely three years later, Statista another online statistics company reported that in the third quarter of 2009, smartphone shipments tallied at 173.5 million units globally [36], demonstrating the extensive growth of these devices. Broken down into operating system platform, the report showed that iOS had a global smartphone sales market share of 17.1 percent [37] whilst BlackBerry had achieved sales of 20.7 percent. However, these high market share figures shared between iOS and BlackBerry were transitory, as these platforms were soon to be dwarfed by Google's Android mobile operating system which was commercially available for the first time in 2008 and will be discussed in the following section.

Google Android

Google's Android OS, which is based on the popular open-source desktop operating system, Linux is developed and maintained by the Open Handset Alliance (OHA), which is a collaboration of technology companies that include mobile operators, handset and component manufacturers as well as software developers [38]. Leading search engine company, Google, whom are the primary driving force behind OHA, acquired Android from an upstart company of the same name in 2005 [39].

Unlike iOS and BlackBerry, which are both proprietary mobile operating systems exclusive to the device hardware manufactured by their respective parent companies, Android, marketed by Google as an open-source mobile operating system was designed to be used over a range of different hardware, most popular on devices which use Advanced RISC Machines' (ARM) [40] processors as their CPU. Hoog [39] writes that most, if not all Android devices utilize ARM processors which are primarily designed with minimal power usage and heat reduction in mind [41] allowing for less bulkier battery and cooling options as compared to desktop and laptop computers. These are the primary reasons for ARM's dominance in mobile devices which allow manufacturers to produce a device with a much smaller physical profile. There are however cases where enthusiasts and technology companies have ported the operating system to work with other traditional x86 processor architecture such as those designed by Intel and AMD.

The first Android mobile device, the HTC Dream 100 was released in October 2008 [39]. The device operating system was designed to be used with online functionality and therefore used both Wi-Fi and cellular data networks as options for connection to the Internet. Standard features also included the ability to make and receive phone calls and short message service text messages (SMS) and also included a built-in HTML web browser, GPS connectivity, email client and most importantly, the ability to extend the device functionality by installing applications from Google's official software repository, then known as the Android market.

What was also notable with the Android operating system was the ability and freedom for users to store data on their devices via on-device local storage mediums such as removable memory cards [39]. Local data storage has long been standard functionality in traditional desktop operating systems and this offered users immediate advantages over iOS, while at the same time closing the gap between smartphone and desktop operating systems even further. Later versions of iOS and the associated devices also improved the options for local storage and it is common for smartphones and tablets to have local device storage within a range of anything between sixteen gigabytes (16GB), up to one-hundred and twenty-eight gigabytes (128GB), which allows storage of significant amounts of digital information. The ability to store private data on device local storage of course establishes direct security implications owing to the fact that smartphones and tablet computers are easily lost or stolen when compared to desktop machines solely because of the smaller form factor.

As the major mobile platforms matured, it was realized that third-party application development was a key factor for platform success [30]. Android achieved this in a similar manner to other mobile operating systems by providing free development tools and *device independent* API's for software developers to create applications. Applications written in Java, are then made available for download from Google's official application repository, the "Android Market" now known as the Google Play store [42]. Unlike Apple, Google developed a more flexible operating system and devices were not restricted to download applications exclusively from the official repository. As a result, many unofficial Android application markets exist. The advantage of this is that third-party application developers have more options for software distribution. The disadvantage however is that the uncontrolled nature of unofficial markets has affected the platform's security reputation, a discussion of this continues in Chapter 3.

Google's mobile operating system proved highly popular since the original release and many major device handset manufacturers started adopting it as the preferred platform on their smartphone and tablet devices. These included mobile handset makers Samsung Electronics, Motorola Inc, LG Electronics, Sony Ericsson and even non-mobile phone technology companies such as ASUStek and Acer which are also part of the OHA [38]. Statista reports that in first quarter of 2011 Android had surpassed all other mobile device platforms [37], replacing Symbian as the market leader with 36.4 percent versus 27.7 percent overall smartphone market share. This number continued to increase and by the end of 2011 Android's growth had risen to 50.9 percent of the overall smartphone market.

The most recent major release of Android at the time of this writing, version 5, codenamed "*Lollipop*" was released in late 2014 and was the first smartphone operating system to offer native support for multiple user accounts [43]. This indicates the device platform showing signs of maturity with enterprise-like features and may even have potential for future use as a replacement for current popular desktop operating systems in low-powered, less processor intensive business usage scenarios that still require the speed advantages offered by keyboard and mouse input methods. This realization could be intensified especially if users wanted to carry the Android smartphone user experience over to the desktop, which is likely considering the platforms large user base and popularity. An example of such a device, the CloudGate Android PC[4], designed by local South African company Cloudware Technologies is already commercially available [44].

Android's growing popularity has also appealed to malware writers which is discussed in more detail in Chapter 3. Despite this, the user base continued its growth, as the operating system has

[4] http://www.cloudgate.co.za/what-is-it/

proved hugely popular globally as well as locally in South Africa. Android offered users more freedom in terms of operating system customization than any mobile operating system before it and when combined with Google’s software ecosystem of online cloud-based applications and storage, it is not difficult to understand the reasons for this popularity.

2.2.2.4. 2011 onwards

Microsoft Windows Phone OS and Windows RT

With origins as far back as early 1997 with Windows CE, one of Microsoft’s first mobile operating systems [45], the software company’s mobile operating systems have a long history. After Windows CE, Microsoft continuously developed a long list of Windows Mobile operating systems, through to Windows Mobile 6. As these operating systems did not have a major impact on consumer or business markets, mentioning all of these would be beyond the scope of this study.

In 2011, following the success of Google and Apple, Microsoft noticed that smartphone and tablet PC’s sales were increasing in momentum and similarly decided to increase development for their own mobile operating system. The software company has a long history in both consumer and enterprise markets with its desktop operating systems and recently made a push for success in the mobile market. The company decided to partner with Nokia [29], the only major mobile device manufacturer that had not adopted the Android operating system due to its previous investments with Symbian, making Windows the principal operating system of choice for the company’s smartphone line of devices. The differences when compared with Apple and Google’s offerings are not significant enough to go into detail, with smartphone operating systems by this time already having a fairly standard and similar feature set.

Windows Phone OS and the tablet PC version, Windows RT, are licensed by Microsoft for use on various hardware platforms, which show a similar model to Google’s Android. The company also freely provided a Software Development Kit [46], as well as relevant documentation for third-party application developers. Similarly, to Apple’s iOS, Windows Phone application developers are only provided the option of publishing their applications via Microsoft’s Windows Phone

Marketplace. Unofficial software repositories currently exist for Windows Phone, but similarly to iOS, the device need first be jailbroken before these can be used as application installation sources.

According to Information Technology research firm Gartner's global smartphone end-user sales report, in the second quarter of 2012 Microsoft had sold just over 4 million devices while the closest competition being BlackBerry had sold almost 8 million devices. The following year in the second quarter of 2013, BlackBerry sales had decreased to just over 6 million, while Microsoft sales had increased to over 7 million units. In contrast, Apple's iOS devices had sold over 31 million while Android devices had figures of more than 177 million units sold in that same period [47]. The report lists other available mobile devices but the device count sales numbers are not significant enough to mention.

2.2.3. Summary

Computing technologies have physically transformed from large computing servers and mainframes, down to much smaller personal computers and even smaller eventually into mobile computing handheld devices. This broadens the range of devices and operating systems IT Departments now need to establish controls and policies for. The shift toward mobile computing has also been assisted by supporting mobile broadband technologies such as Wi-Fi and 3G mobile data networks which broaden the support scope even further by allowing access to information from almost any location at any time.

Similar to the evolution of computer use from mainframes to personal computers due to advancements in technology, both the hardware and software of current smartphones and tablet computers have advanced in recent years to such an extent that they are being used for computing purposes that were originally only possible on traditional personal computers. In a recent report in July 2014 according to Google, its Android mobile platform has over one billion active users per month [48]. A month earlier in June 2014, Apple announced that a total number of eight hundred million iOS devices had been sold to date. This number was up from six hundred million the year before [49] in June 2013. These figures not only show the pervasiveness of these devices but also show continuous growth, increasing the likelihood that smartphones and tablet PC's will be used to access work related information or be directly connected to company networks by employees.

For this same reason it is very likely for university staff and students to want to use them to access educational resources as well. The devices that are current include RIM Blackberry, Apple iOS, Google Android and Windows Mobile, with Symbian devices now falling into the legacy category.

The widespread user base, in combination with technology advancements that have allowed smartphones and tablets to become handheld computing devices, illustrate that it is worth assessing the risks associated with mobile devices. The direct benefit of having continuous access to information from these devices increase the likelihood of employees using them to access work-related private information. As such it is important that information security controls are established to mitigate any risks associated with the use of personally-owned mobile devices when accessing business related information.

2.3. Current Practices

As mentioned previously, the capabilities of today’s mobile devices have extended their usability into a class of computing technology previously restricted to personal computers and are thus being used for both personal as well as work related purposes. Personal computers developed in a similar manner into information sharing systems and are now critical business tools. This convergence from personal to organizational use is not surprising given the advantageous capabilities of smartphones and tablets. For users, the benefits of mobile computing are easily recognized and users would prefer to carry a single mobile device instead of carrying multiple devices for both private and business purposes [50].

There are however also disadvantages for personal, and more importantly in the case of this study, organizational use of current smartphones and tablet computers. The information security and privacy risks are less obvious and are usually only observed at the occurrence of incidents, such as a security breach which results in loss of confidential business information. Some of these concerns have already been highlighted by security researchers. Examples such as the “Find and Call” trojan application previously found in both iOS and Android official application repositories which was designed to leak device contact information [51], and the growing number of samples of malware found on current mobile platforms give evidence of the validity for the concerns [52].

These cases have been the focus of many technology-driven online articles and academic research papers. Despite this, because of the beneficial computing capabilities and popularity of these portable computing technologies, there is an indication of increasing organizational use by employees regardless of valid security concerns.

In the previous chapter, market share figures were used to portray the pervasiveness of smartphone and tablet use. These figures however do not give actual evidence of device adoption within organizations. This chapter provides an introduction of such evidence to establish relevance of the extent of mobile device use within organizations.

2.3.1. Organizational Use of Mobile Devices

In a paper by Lebek *et al.* [53] which investigates influences of employees intention to use mobile devices in a BYOD context, the author suggests that people in the workplace are generally motivated to use systems that assist them when performing their jobs. The researcher goes further to describe a technology acceptance model (TAM) derived from previous research that suggests that perceived usefulness of a technology has a significant positive effect on people's intentions and that these intentions are formed towards behavior's that are believed to bring an increase in their job performance. This hints at the reasoning behind the desire of employees wanting to use smartphones and tablets for business use.

Technology companies have also started directing their business focus toward mobile computing technologies to keep up with this trend. In February 2014, incoming Microsoft CEO stated in an email to Microsoft employees "*Our job is to ensure that Microsoft thrives in a mobile and cloud-first world.*" [54]. The significance of this statement is that it comes from a software company, which is arguably the global technology leader in terms of Personal Computer operating systems for both consumers as well as enterprise use. Microsoft's business model is greatly centered on the company's desktop operating system Microsoft Windows which still holds the majority of market share within its class of personal computer operating systems. This statement nonetheless hints that the company has realized the growing demands for mobile computing and has made the observation that future innovations for its software should consider incorporating mobile features.

In 2011, information security research firm Goode Intelligence conducted a mobile device survey covering various security related themes [55]. One-hundred and thirty respondents took part in the survey and were a mix of Information Security and IT Management professionals from government, healthcare, finance, technology and manufacturing industries globally. This was the third survey of its kind conducted annually by the company. One of the key findings from the survey was that 71 percent of the respondents stated that their organizations allowed personally-owned mobile devices to be used for company business, meaning that this practice occurred at just over two thirds of the surveyed companies. The results of the previous year's findings were also just over two thirds, proving that the figures were consistent and that a fairly high percentage of organizations allowed this.

Further analysis from the 2011 Goode Intelligence survey examined mobile adoption to determine the dominant mobile platforms used in organizations [55]. They had found that, the use of Symbian was present in 24 percent of the surveyed organizations, 41 percent of the surveyed organizations used Windows Phone, 65 percent Android, 70 percent BlackBerry and 77 percent used iOS. Of particular interest, Google's Android was only present in 16 percent of organizations from the survey done by the company in the previous year showing a sharp rise in Android organizational use in 2011. This coincides with the previously discussed Statista market share report when the Android platform showed a sharp increase [37] and thus strengthening the premise that consumer mobile device popularity increases the likelihood of organizational use.

2.3.2. Organizational Use of Mobile Devices within Universities

While educational institutions were overlooked in the Goode Intelligence survey, an indication of mobile device adoption in universities is presented in various reports. As an example, Long Island University in the United States begun a pilot program in 2010 which provides Apple iPad tablet devices to incoming students as well as academic faculty members [56]. The cost of these devices are included into first year student fees and existing students are allowed the option to purchase the tablets at half price. The CIO and project manager of the initiative mentions that one of the primary goals was to use the tablets as a replacement for traditional textbooks but the main barrier to accomplishing this was that the publishing platforms and textbook industries have not yet agreed on a standard for doing so. It is believed that this will happen in the near future but in the meantime, they are finding the devices useful in other ways.

The use of an iOS application called iSeismometer is one such example. A graduate student from Long Island University's Earth Science faculty created iSeismometer for the purposes of conducting academic research. The App uses the iPad or iPhone device's built-in accelerometer to collect seismic data for later research [56]. There are traces of the application's use in other medical academic literature as well. In a recent medical academic journal, iSeismometer is used to measure neuromuscular functions in patients [57]. This demonstrates the versatile use cases for mobile devices across a range of educational disciplines to facilitate learning, making the appeal for widespread use across higher education apparent.

Within South African university institutions, a similar drive toward personally-owned laptop and more importantly tablet PC use already exists. The Student Technology Program (STP)[5], which is an initiative negotiated by the Association of South African University Directors of Information Technology (ASAUDIT) offers students and staff from South African public universities affordable deals on laptop and tablet PC's. There are instructions on ASAUDIT's web site of how to place orders and a list of available devices, which include a range of Windows as well as Android tablets.

2.3.3. Summary

This chapter provides evidence that smartphones and tablets are being used globally both in industry by employees as well as by students in universities for various purposes. Unlike in the past, where IT Departments were chiefly in control of device procurement, the use of these technologies are motivated for by the users themselves, Disterer and Kleiner [50] refers to the practice as "user-driven innovation". These examples of business use of personally-owned mobile devices clearly show the extensive advantages for their usage and why employees or students would want to leverage these benefits.

[5] http://www.stp.ac.za/what-is-stp.html

The benefits of personally-owned mobile devices for organizations include increased user adoption of technology and reduced hardware costs benefits. Organizations also benefit from increased user availability with devices being mobile and as such, users are able to retrieve business information from almost any location. Lastly, mobile devices offer flexibility for both staff and students in university environments allowing users the option to choose their own tools which ultimately increases productivity. What is not entirely clear, is if the users or organizations are aware of the risks introduced to their organizations by the practice of BYOD.

2.4. Conclusion

Current practices reveal that the use of mobile devices within both other organizations and universities have recently rapidly increased and that the choice of device is being driven by the end user. The reasons for this are the productivity benefits that university staff and students get from current smartphones and tablet PC's. Device portability and usability are the core benefits of current mobile devices and this facilitates learning and offers users continuous access to information.

Universities, as institutions have a culture of sharing educational information. This sharing amongst support staff, lecturers, visitors and students is supplemented by mobile devices because they allow continuous access to educational and work-related information. However, universities also collect enormous amounts of sensitive digital information that should have restricted availability. The leakage of such information could result in reputational and financial damage to the institutions and thus it is essential that the necessary strategies are implemented to minimize this risk.

While the advantages of using personally-owned mobile devices for universities are easily recognized, the contrary is that mobile devices increase the risk of data leakage by increasing the complexity of configurations for IT Departments and Information Security professionals alike.

Chapter 3 – Technical Discussion

While mobile devices create complexity for IT Departments, additional threats and vulnerabilities are also introduced into organizations which amplify data loss concerns. These threats and vulnerabilities and their implications are discussed in the following chapter in order to understand the additional risks that are engendered by smartphone and tablet PC's. Some examples of mobile device malware on each of the current mobile device platforms are discussed in chronological order, as well as the exploitation trends attackers are currently using to gain unauthorized access to mobile devices.

3.1. Mobile Device Malware

There are many organizational concerns presented by the use of personally-owned mobile devices for business. There are legal, financial and data security implications that need be considered [58]. Legal implications, such as considerations related to POPI; financial implications, such as the purchase of hardware, software, network infrastructure and IT staff training to manage the increased support raised by mobile devices; and security implications which relate to threats to the confidentiality, integrity and availability of sensitive business data. The financial and legal implications, although interrelated, are beyond the scope of this research and are briefly reflected upon where necessary, but the greater part of this study focuses specifically on the security related concerns. While laptops are also considered mobile devices, the threats and device control techniques have already widely been covered in literature, hence this research focuses on smartphone and tablet PC technologies.

In order for organizations to minimize risk and implement security controls related to managing these mobile devices, it is first important to understand what the security weaknesses and concerns are. The following chapter reports on these mobile device weaknesses and how they may be exploited by cyber criminals through the use of malicious software. Attackers have successfully used Viruses, Trojans and Worms on traditional desktop operating systems for many years to leverage attacks from workstations to obtain important information from attached network systems. As such, this chapter explores malware on mobile devices to determine the severity of the threat which could similarly be used as a gateway to obtaining information from organizational network systems that are connected to user-owned mobile devices.

3.1.1. Mobile Malware Evolution

Malicious software such as viruses, worms and trojans are commonly known by the collective term Malware. In a wide-reaching definition Vacca [10] describes malware as software that is designed to penetrate or damage computer systems without the owner's informed consent. This echoes many statements found in generalized information security literature such as within the book this statement comes from. In the beginning of the PC era, malware was not originally designed with malicious intent or for financial profitability. Hypponen [59] writes that "…old-school malware written for glory has given way to a new era of crimeware designed for spamming, data theft or extortion". Crimeware is defined by Vacca [10] as economically motivated malware. Hypponen's statement indicates that there is evidence of malware evolving for economically motivated criminal purposes and theft of information. Such malware was typically only found on traditional desktop and laptop computers but is now also common on smartphone and tablet devices.

The following section provides a malware timeline analysis for each of the mobile platforms that demonstrates the burgeoning problem of malware on mobile operating systems similarly to how it has been an established as an ongoing threat for traditional PC operating systems. This is revealed by analysis of the various reports of malware and their behaviour which are found on mobile operating systems to determine the scale of mobile malware trends.

3.1.1.1. Palm OS

The palm line of handheld computers was introduced in 1997 and around mid-2000, the device operating system received the first publicly exposed reports of malicious applications targeted at Palm OS. Malware in the form of a Trojan-Horse named 'Liberty' was reported in August 2000 [24][28] which would delete installed applications from the device. A month later in September 2000, a virus named 'Phage' was reported to infect device applications and make copies of itself on the device’s local storage. A significant design limitation with Palm OS when compared to more recent mobile device operating systems, was that third-party applications could only be installed onto the device by synchronizing with a local user desktop computer. This constraint also meant the only way for Palm malware to spread to the devices was also via local synchronization with the user’s workstation.

As a result, Palm OS did not make for a particularly attractive proposition for malware writers as it effectively limited the spread of device malware due to the necessity of locally connecting the devices to their traditional desktop machines each time. As such Palm malware was not able to spread freely between devices as compared to desktop malware at the time.

3.1.1.2. Symbian

The rise in popularity of the Symbian OS platform around 2004, as discussed previously, attracted the interest of malware developers and the operating system also became the new target for mobile malware.

In 2004, security researchers identified Cabir, a worm which was originally a proof of concept. According to Hypponen [59] Cabir was the “first rogue program written specifically for smartphones”. Coursen [60] confirms this by making the statement that Cabir was the first malware to run under the Symbian operating system. The worm, in its original form, had no additional payload and did not do anything malicious other than its propagation technique which is what made Cabir noteworthy. It initially used Bluetooth as the primary propagation method and this, the first of its kind, effectively removed the chains of limitation for malware proliferation experienced with Palm OS before it. Cabir appeared at a time when Bluetooth was the primary method for data transfer between mobile devices [61]. The only harm caused by Cabir was reduced battery life due to the worm’s interference with Bluetooth functionality, causing the infected device to constantly open Bluetooth connections with other devices within range in an attempt to copy itself to other Symbian phones. Other more damaging variants of Cabir were thereafter discovered after malware writers started modifying the original version.

Leavitt [28] mentions that the most worrying scenarios around malicious mobile software was not malware written by inexperienced hackers, but by organized criminal groups. This statement gives us a hint toward the changing nature of the information security landscape at the time. Continuing this sentiment, Leavitt then states that the principal driving force behind mobile malware is for financial gain. Mquito [28], also targeted at Symbian series 60 devices, showed evidence of this as the malware abused SMS functionality to send text messages in the background without any user intervention to high cost premium-rate phone numbers across Europe, running up the user's bill in the process.

Symbian market share kept growing throughout the early to mid-2000's along with its popularity for malware. Between July 2004 and July 2008 more than 290 Symbian related malware samples were reported in the wild [62].

3.1.1.3. BlackBerry

Similarly to Symbian, malware writers started taking notice of BlackBerry's increasing user base to which the company responded by introducing a security model which implemented limitations to any third-party applications that attempted to access the system protected API's of the operating system. BlackBerry, required that third-party application developers digitally sign applications with a cryptographic key pair, provided by RIM. A similar idea was introduced into the latter years of the Symbian operating system when research indicated that mobile malware was on the increase.

BlackBerry OS had developed a reputation of being a secure mobile operating system, but in 2006, a security researcher demonstrated the ability to attack hosts within the internal business network via BlackBerry devices that were connected to it [63]. This indicated that BlackBerry devices were similarly vulnerable, when compared to the Symbian platform before it, although reports for malicious software on the platform were minimal.

In 2011, malware security researchers at Trend Micro [64] discovered spyware targeted at the BlackBerry OS named BBOS_ZITMO.B of which variants for Symbian OS and Microsoft's Windows Mobile were also discovered. The code showed a variant of ZeuS, malware that was initially intended for the PC. BBOS_ZITMO.B would run silently in the background without any user interface indication of the device being infected. After being installed successfully, a confirmation is sent to the attacker via SMS indicating that the malware is ready to receive commands. The attacker is then able to use the malware to issue various commands, of which the primary objective is to steal information by getting the malware to forward text messages from the device to a mobile number of the attacker's choice.

Of note, in a 2011 paper written by Mylonas *et al.* [26], the authors mention that for applications submitted to be published in the official BlackBerry repository, the code is not evaluated for signs of malicious behaviour. BlackBerry also does not provide a means to remove malicious applications which may be discovered after installation from devices. For these reasons, the authors are of the opinion that the BlackBerry application repository appears to have the least security controls [65].

RIM's BlackBerry operating system was not plagued by mobile malware and remains this way today. For this reason, the online reports and academic literature on the subjects occurs to a lesser extent than other mobile platforms. The reasons for this are largely due to the platforms smaller market share, nevertheless these reports show possibilities of malware occurrences on the BlackBerry platform.

3.1.1.4. Apple iOS

Apple's iOS, which pointed out previously has a relatively large user base, has to date had very few reported cases of rogue applications with malicious behaviour slipping through Apple's testing process and ending up on the official "*App Store"*, software repository.

There is a high probability that Apple initially had the intention of limiting their device's third-party software install options exclusively to their official software repository to prevent application piracy but this has proved beneficial for security reasons as well. iOS' security model only permits applications which have been digitally signed with certificates issued by Apple onto the App Store [66]. What makes Apple's security model unique is that before each application is signed, it has to go through a human vetting process to test for functionality consistency as well as for any malicious behaviour [26]. This process has proved fairly successful so far, as malware on iOS devices have been kept at a minimum.

In one of the earlier cases of iOS malware history, security researcher Maslennikov [51] discovered an app named "*Find and Call"* that appeared in the App store in 2012. This was reportedly the first known occurrence of malware in the Apple's software repository, 5 years after the initial iPhone launch in 2007. The application, which was subsequently removed after being reported to Apple, claimed to have functionality that assisted the user with finding contacts when in fact it would instead upload the device contacts list to a remote server when launched. Since the application's functionality was remarkably different from the original claims, "Find and Call" was considered a trojan.

Apvrille [67], recently produced a consolidated list of all the iOS malware instances, of which there are eleven in total and eight of these only work on jailbroken devices which allow the malware to be installed from unofficial application repositories. The most recent case of iOS malware was discovered in November 2014 by security company Palo Alto Networks. A new family of malware named WireLurker [68], targeted both iOS and Apple's desktop operating system. OS X differs from iOS by allowing software installations from unofficial software repositories by changing the default operating system security settings. WireLurker was found in 467 trojanized applications on a third-party OS X App Store in China and once installed, facilitated infection of iOS devices via USB connection to the desktop PC by exploiting a vulnerability in the mobile operating system. What was significant about WireLurker was that it is able to infect iOS devices that are not jailbroken. It must be noted that while having the advantage of being able to infect any iOS device, the chances of malware distribution are diminished by the necessity of having to be tethered to a desktop PC with OS X before infection is able to take place.

This proves that there exists rare cases of malicious software even within Apple's curated App Store model, but the threat has been minimized because of manual application vetting. Egele *et al.* [69] however has valid doubts about the protection of user data in third-party iOS applications because the exact details of the Apple's testing processes are not publicly known and user or organizational trust is hereby completely placed in the vendor. To test information leakage in iOS applications, they developed a static analysis model and analyzed over 1,400 iOS applications. The results showed while the majority of applications leak the device ID, only a small amount of these actually leak more useful personally identifiable information.

While malware on iOS has been minimized, other reported cases of attacking Apple's mobile operating system do exist, with researchers directly exploiting software vulnerabilities instead of using malicious software, examples of this will are discussed in Section 3.2.

3.1.1.5. Android

Android's popularity has placed a huge target on itself for malware. In the past, in terms of desktop operating systems, a similar trend can be noticed. For example, Microsoft Windows, which has been and currently still is the most prevalent desktop operating system, is by far the most popular target for malware writers due to its wide reaching user base. Android device proliferation is certainly one of the key reasons for the platform's subsequent malware interest, although there are other theories that can be drawn upon from Android's methods of application distribution.

For instance, Android provides a SDK, which is free and publicly available with documentation and tools for application developers to create applications with the Java programming language. The installation package file (.apk) for every Android application installed on user devices must be digitally signed with certificates of which the private key is held by the developer. The software developer's digital signature is then mapped to the application's unique ID [26]. According to the official Android documentation [70], a developer has the option to self-sign their certificate as it is not compulsory to sign applications with certificates from a trusted certificate authority. As a result, the majority of Android applications are self-signed. Without going into much detail, this means that because the certificate is not verified by a trusted third-party, it is really up to sincere developers themselves to maintain security of the private key. Furthermore, the certificate not being verified keeps any potential attacker anonymous as well [26]. It could therefore be suggested that knowledge of this provides encouragement to malware writers as they would not need to go through the drawn out process of first registering with a trusted certificate authority.

Android developers also have the option of application distribution via either the official software repository, the Google Play store, or via third-party software repositories, an example of one such repository is the Amazon Appstore for Android[6]. In a 2011 journal article, Mylonas *et al.* [26] notes that Google does not employ human vetting to test the applications which are submitted by developers for distribution via the official Google Play Store for malicious behaviour [26]. Instead, based on negative user ratings or direct reports of malicious software, Google addresses malware found in the Play Store with remote uninstallation functionality which is built into the Android operating system [71], thus being a more reactive malware management model as compared to the proactive approach used by Apple.

Discussing security in application markets McDaniel and Enck [72] state that "markets entice developers by placing low economic and technical barriers to entry, thereby fostering fast-paced innovation". This statement suggests the advantage of Android's approach in that it enables third-party developers to develop applications more rapidly and thereby growing the software repository faster. The more applications available for a specific mobile platform, the more useful the platform becomes giving it a commercial advantage. Both Apple and Google have many times used this as a marketing tool[7] to suggest superiority for their respective mobile platforms. The disadvantage is that this provides even more encouragement for malware writers as it is easier to publish malicious applications in the Android software repository. It is a well-known theory amongst information security professionals that cyber criminals choose soft targets which provide maximum prospective gain.

The option to install applications from informal software repositories can be contrasted with a model more akin to desktop operating systems. The difference being that desktop operating systems have matured for enterprise use and allow multiple user accounts which allow restrictions to be placed on standard, less privileged user accounts versus administrative, full control user

[6] http://www.amazon.com/gp/mas/get/android

[7] http://techcrunch.com/2014/06/02/itunes-app-store-now-has-1-2-million-apps-has-seen-75-billion-downloads-to-date/

accounts. A secure business desktop configuration would place limitations on the installation of software from ordinary user accounts onto organizational computers. Current smartphone operating systems are designed with only a single user in mind and until now, such detailed control has not been possible.

In 2012, Google announced the use of a service named Bouncer [73] which automatically scans the Android market for applications in the Google Play store that show signs of having known malware signatures. While not being as thorough as a manual vetting process, Bouncer does help to remove most of the unwanted known Google Play store related malware created by less skilled malware developers.

Before the Bouncer update, in August 2010, two years after the first Android device went on sale, Kaspersky researcher Dennis Maslennikov reported what is known as the first SMS trojan for Android, named “FakePlayer” [74]. The trojan, which appeared as a media player application would send SMS messages to premium rate mobile service numbers without the user knowing. FakePlayer had very similar characteristics to the Mquito trojan for Symbian devices discussed earlier.

In the same month, spyware named “GPS Spy”, which exploited Android’s GPS capability was identified. This was also a trojan, and would send the device GPS coordinates details to a remote server without the user knowing [74]. GPS Spy was considered low-risk, because the propagation technique required physical access to the device. Its significance was that it demonstrated an exploit not seen before on any smartphone or computing device.

Of particular importance, toward the end of 2010, another trojan named “*Geinimi”* was discovered, which would forward personal information collected from the device to a remote server. The significance of Geinimi was due to the innovative propagation method. The malware would infect known legitimate applications by repacking them with malicious code [61] which were then later found distributed on unofficial application repositories as well as file-sharing websites. The anti-malware company Lookout Inc., whose business focus is on mobile malware, discovered Geinimi and were calling it the most sophisticated Android malware to date [75], noting that it was also the first evidence of mobile malware to exhibit botnet-like capabilities, displaying the potential to receive commands from a remote server. Botnet’s are common threat to traditional computers and networks and are largely responsible for spam and distributed denial of service attacks (DDoS) [74]. Geinimi was however never found in the official Android market.

Many more Android trojan applications appeared in unofficial application repositories from 2011 onward and the foremost security recommendation was to advise users to only install applications from reputable sources [75] or configure their devices to change the security settings to not permit installation of apps from unknown sources. These recommendations would soon lose merit, because in March 2011, another trojan named DroidDream had been reverse engineered by malware writers into over fifty legitimate applications, repackaged and published on the official Android market [71]. Alarmingly, the count for the amount of users infected exceeded 260,000 within forty-eight hours before Google eventually pulled the malware from the Android market [76]. DroidDream was considered high risk malware, because it enabled an attacker to obtain device root privileges and thereby allowing full remote control of the smartphone by using publicly disclosed Android exploits such as RageAgainstTheCage [61]. After the discovery of DroidDream, researchers discovered DroidKungFu which displayed almost identical characteristics to DroidDream, the difference being that the malware encrypted the exploits to avoid detection from mobile anti-virus software. Another key difference was that DroidKungFu was only found in unofficial Android markets.

In the same year of the DroidDream discovery, another trojan by the name of Plankton was identified. Plankton, by means of basic remote commands allowed an attacker to change the mobile browser homepage, add bookmarks and news shortcuts to the device and also steal browser history and device information which it would then upload to a remote server [77]. Apvrille [52] states that Plankton is still found in a large number of applications on the Google play store and to date has infected more than five million devices.

In 2013, the first known Android targeted attack was discovered and made use of malware named Chuli [52]. During the World Uyghur Conference held in March 2013, the email account of a high profile activist was used to target the email accounts of other human rights activists. What made this attack unique, was that the emails included an Android application package (.apk) file attachment which contained a copy of the trojan [78]. Chuli was designed to collect incoming SMS text messages, device contacts, location information and recorded phone calls and then send this information to a remote server.

Apvrille [52] states that in 2013 more than 1300 new malicious applications were being discovered per day and current anti-malware systems are tracking more than 400,000 malicious Android applications which contain over 300 different Android malware families. The reality is that mobile malware is increasing in numbers and targeted predominantly at the most popular mobile platform, Google Android. Various academic literature as well as online reports confirm this. The reason for this is mainly because of the user pervasiveness of Android, but also because of the less stringent controls Google places on developers such as allowing applications to be self-signed, less strictly tested or by allowing applications to be distributed on unofficial application repositories.

When compared with other current popular mobile platforms, such as iOS which tightly controls which applications are allowed onto the App Store, it is understandable from the perspective of malware writers why the efforts are focused on the Android platform. Many of the online reports however stem from anti-malware security vendors which express Android’s malware in great numbers and should be evaluated carefully as these vendors have obvious incentives to promote sales of their software.

A strong concern highlighted by the presented evidence however is that mobile device platforms do not have standardized application submission rules for developers to distribute applications from the respective platform’s application repositories. These rules vary from platform to platform, from strictly controlled application submissions, to relaxed rules which rely on malware discovery after submission. While other platforms do not report as much mobile malware as Android, the vast majority of Android malware is found in the form of ‘trojanized’ versions of legitimate applications on unofficial third-party application repositories. The Google Play store is by no means malware free but the majority of the reported cases were eventually removed by Google after discovery. This however still leaves a significant window of device infection for Android devices until malware is reported and ultimately makes the platform less safe with regard to malicious software.

For these reasons, a strong recommendation is that users are advised or not allowed to ‘jailbreak’ or ‘root’ their devices and only install applications from official application repositories. Organizational policies or best practice recommendations would need to enforce this behaviour. Such policies however do not protect users against less governed official repositories, of which the only current worthwhile defense is to educate users to be vigilant about checking application permission requests and application reviews prior to installation. For vendors, establishing standards for mobile platforms that ensure stricter control when applications are published by developers would be a welcomed mitigation strategy.

3.1.1.6. Windows Mobile / Windows Phone

Due to Windows Mobile being relatively new compared to other mobile operating systems, malware research and online reports for the platform are rare. The reason for this is that Microsoft’s mobile operating systems do not currently share the same prevalence amongst users and as such, malware writers are not motivated to devote time and effort to develop malware for a platform that will ultimately only target a small user base. However, it is probable that this will change if the platform popularity increases.

Additionally, Microsoft only allows applications to be downloaded from the official repository and uses application vetting techniques. According to the company, it has stated that every app is tested and reviewed for potential malware and performance issues and certified by Microsoft before being allowed onto the Windows Store [79]. This strategy increases effort for malware developers and given the smaller user base, results in Windows Phone malware currently being unproblematic and scarcely reported.

3.1.1.7. Cross Platform Malware

Most mobile malware is restricted to certain mobile device platforms, however in 2006 a device independent trojan named RedBrowser [52] was discovered that presented a major difference to previous mobile malware. RedBrowser, also sent SMS messages to premium rate mobile numbers, but the difference was in its propagation technique. The trojan would infect devices via the Java 2

Micro Edition (J2ME) platform and because Java is universally supported across all operating systems, it made the host operating system irrelevant and thereby promoting its infection rate.

3.1.2. Summary

As evidenced above, the threat of malware on mobile devices is increasing and is more problematic on certain mobile problems than others for various reasons. Additionally, the recent popularity of mobile devices as computing platforms have exaggerated the interest of mobile malware developers as a means to obtaining access to private information. Similarly to the current trends of malware distribution on traditional desktop PC platforms, the most commonly used mobile malware distribution techniques on current device platforms is to repackage legitimate applications into malicious ones in the form of trojans. The advantage of which is allowing attackers surreptitious remote device control.

While anti-malware solutions for mobile devices are available as viable mitigation strategies, they have a similar limitation to desktop anti-virus products in that the software is only able to protect devices from known previously discovered malware signatures. As such, while useful as an added layer of protection, anti-malware should not be relied on as a complete protection solution. As pointed out by Mylonas *et al.* [26] some of the better and often more cost effective solutions to avoid mobile malware outbreaks are user awareness about the privacy risks and secure application distribution in mobile device platforms. As such, institutions need to adopt a holistic security strategy which includes other types of defenses as well.

3.2. Mobile Vulnerabilities, Threats and Exploitation Trends

While it is clear that mobile devices are susceptible to malware in a similar way that traditional computers are, this is not the only cause for concern. As with all software, vulnerabilities have always existed due to mistakes made by human software developers. Such vulnerabilities have been exploited with mobile operating systems as well.

Mobile threats can be classified into several categories based on the approaches used by attackers. Application-based threats are mostly covered by mobile malware which was more extensively discussed in the previous section. Physical threats include device loss, theft or even exploiting physical weaknesses to gain access to data on a mobile device. Web-based threats include browser-based phishing scams or exploiting known vulnerabilities in web browsers. While these threats are categorized separately, they are often combined in a typical attack and for this reason their degree of exploitation is not emphasized in the following chapter. The following section explores examples of mobile device vulnerabilities and the techniques in use today in which such vulnerabilities are exploited by attackers.

3.2.1. Physical Threats

Given the small form factor and mobile functionality of smartphone and tablet devices, they are inherently more susceptible to physical loss or theft when compared with desktop computers. This ultimately applies to laptop computers as well given their mobility factor. As previously mentioned some smartphones and tablet computer models have removable storage such as memory cards which are easily removed from the device. If these memory cards have any confidential or business related information stored on them, access to this information is easily obtained by using an external memory card reader. This can be mitigated by ensuring device local storage encryption, which is a standard feature today on most traditional as well as mobile device operating systems.

In South African reports, statistics of lost or stolen mobile devices are hard to find but a recent consumer survey done in the United States indicates that in 2013, stolen smartphones were counted at 3.1 million and lost smartphones counted at 1.4 million devices. Interestingly only 36 percent of users actually configured their devices with the most basic built-in security control, the device lock screen pin [80]. In 2011 a survey of 458 smartphone users was done in Greece by Mylonas *et al.* [81]. They discovered that 30.1 percent of the respondents reported that they had misplaced their devices at some stage in the past. Given the high rate of lost and stolen devices it is important that at the very minimum, organizational security policies enforce users to configure their devices to use a Personal Identification Number (PIN) or password-enabled screen locks.

Different mobile device operating systems also have difficult default security configurations for enabling device pattern or PIN locks. The current version of Apple’s iOS for example encourages users to configure the device with a PIN lock during initial configuration assisting iOS users to configure their devices more securely. Android, at the time of this writing leaves this decision up to the user to discover and does not offer this option at initial configuration. On the other hand, Android's security features require users to configure a pattern, PIN or password lock when using certain potentially sensitive features of the device, such as those that allow credential storage. For example, when configuring Android's default VPN client with a VPN profile, which allows users to store their VPN authentication credentials, the device itself must first be configured with any of the three aforementioned security lock methods and requires the user to do so. iOS on the other hand allows a VPN configuration with stored credentials without requiring a device PIN or password lock. To prevent having to enter long company username and password credentials on their smaller, more cumbersome touchscreen keyboards each time a VPN connection is established, users may have a reason to configure the device this way. In such a configuration, if the user has configured a VPN connection into company networks, a lost iOS device now allows unauthorized remote access from the device directly into company networks. Locally synchronized email clients with stored credentials could be accessed in the same way, demonstrating the importance of a device PIN.

Researchers have also demonstrated attacks on device local authentication mechanisms even when screen locking is enabled, provided the device is physically in their possession such as a lost or stolen smartphone. One such example is presented below.

3.2.1.1. Device Authentication Attacks

Different mobile devices use different types of local authentication methods. Passwords are available as options on almost all smartphone operating systems but are easier to mistype on the small keys found on touchscreen keyboards. As a result, and out of convenience, the most commonly used authentication method on touchscreen mobile devices is the 4-digit device PIN code which is the default authentication method on iOS. Munro states that a 4-digit PIN can be cracked by brute-force in approximately fourteen hours or less depending on which tool is used [82].

With the release of Android version 2.2, the password pattern was introduced as an alternative method of device authentication. According to Aviv *et al.* [83], this method has become the primary authentication method for the majority of Android users and contains a pattern space of 389,112 possible patterns. Designed as a graphical password on a grid of 3x3 contact points, users draw a pattern from one grid point to another as illustrated in Fig. 3.1. Restrictions to this method when configuring the pattern are that users must touch a minimum of four grid points, are forced to touch neighbouring grid points, and each of these points can only be used once.

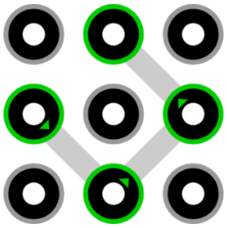


Fig. 3.1 - Android Password Pattern Lock

Aviv *et al.* [83] argues that this method of authentication is not very secure as it is susceptible to 'smudge' attacks whereby the residual finger oil left behind on touch screen surfaces is used to easily guess the pattern lock password and allow an attacker to authenticate onto a device that is physically in their possession. The research concluded that even in situations when pattern lock smudge distortion occurred due to simulated application usage, the pattern was still partially recoverable in 92 percent and fully recoverable in 68 percent of their experiments by using photographs and appropriate lighting. This demonstrates that guessing the Android pattern lock hardly requires any special knowledge or skill, yet is still the platforms most popular authentication method.

Risk: Locally stored data is susceptible to unauthorized access on mobile devices if the device is lost or stolen.

3.2.2. Web Based Threats

Mobile device operating systems are designed to be constantly connected to the Internet and more often than not make use of Internet-based applications and services. The devices are therefore subject to similar web-based threats as those faced by Internet connected personal computers as discussed below.

3.2.2.1. Social Engineering Attacks

Phishing, is defined by Vacca [10] as “the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication”. Social engineering remains one of the more effective methods of persuading computer users to divulge sensitive information or even install malicious software on their own machines [84]. While this type of attack is traditionally and more commonly distributed via spam email, ‘Smishing’ or SMS Phishing is a derivative commonly targeted at mobile devices [85], where the victim receives a targeted, or spam message to their mobile devices via text message. The text message usually contains a link to a malicious website that has the same look and feel of a legitimate site where users are asked to provide their login credentials.

An example of how this is used in combination with operating system vulnerabilities was presented in July 2014 by Xue *et al.* [86] when they discovered the ‘Masque Attack’ vulnerability in iOS which allows a malicious application to replace any legitimate application, that was installed from the App Store, as long as both applications used the same bundle identifier. According to the researchers, the vulnerability affected both jailbroken and non-jailbroken recent iOS versions from 7.1.1 through to 8.1 and affected any application installed on the device except preinstalled iOS applications such as the mobile Safari browser. The attack was demonstrated by luring the potential victim to click on an Internet link in an SMS text message to install an updated version of a specific mobile application. In the example the popular mobile game ‘New Flappy Bird’ is used as a lure. The link then forwards the victim to a website with the fake application which has the same bundle identifier as the genuine Gmail application. If the victim falls for the phishing attack and follows the Internet link, the mobile browser offers an install option to the victim which installs an application of the attacker’s choice over the original Gmail application. In the example, the attackers developed a malicious application with an identical icon and user interface as the legitimate Gmail application to effectively masque the installation of the application. The victim is completely unaware that a malicious application which appears to be Gmail is then installed onto the device by making use of the bundle identifier vulnerability. Thereafter, locally cached emails from the Gmail application, which are stored in clear-text in a local device database is uploaded to a remote server. Any information from the users Gmail account would now be accessible by the attacker.

This attack is noteworthy because not only does this demonstrate how attackers are able to leverage SMS Phishing attacks via mobile devices, but particularly demonstrates that iOS is vulnerable to malicious software installation via avenues which completely bypass Apple’s curated App Store, by combining flaws in the operating system with social engineering. The recommendation here is still the same as for any malicious applications. Do not allow installation of applications from anywhere else other than official application repositories indicating that a strong emphasis on user awareness is necessary.

Risk: Mobile devices are susceptible to remote malicious software installation, thereby enabling attackers to leverage the devices to gain further access to locally stored information.

3.2.2.2. Browser Based Attacks

The Webkit engine which is used by the web browsers of iOS, Android and BlackBerry has several vulnerabilities that have been targeted by attackers. While application-based attacks such as mobile malware require users to knowingly install infected applications onto their devices, browser-based attacks also known as ‘drive-by downloads’ [87] only need users to browse to an infected website for the malware to be automatically downloaded onto the device. Jayasinghe *et al.* [88] states that “These attacks usually leverage web browser vulnerabilities in order to hide malicious software downloads onto a computer or mobile device”. In this scenario, the attack methods originally used on traditional computing platforms have again been adapted for mobile devices. A team of researchers developed an exploit using a Webkit vulnerability and demonstrated the possibility of this attack on an iPhone 4S in 2012 which enabled them to retrieve the contacts, photo’s, video’s and browsing history from the device [89].

The key point to take away from this attack was that known software vulnerabilities were used. The National Institute of Standards and Technology (NIST) keeps a publicly accessible National Vulnerability Database (NVD) [90] of discovered vulnerabilities such as these which are searchable by unique Common Vulnerabilities and Exposure Identifiers (CVE-IDs). For this reason, a particular vulnerability is easily known to both security professionals as well as attackers and identifies which operating systems are affected. The most effective mitigation strategy against this is to ensure that mobile operating systems and applications are regularly updated with the latest versions of the software as these known vulnerabilities are usually patched in software updates by the vendor before being publicly disclosed. Without regular updates, devices are effectively more susceptible to attack as the known vulnerabilities become publicly available.

Risk: Mobile devices are susceptible to operating system and software vulnerabilities in a similar manner that traditional computers are, enabling unauthorized access to remotely stored data.

3.2.3. Summary

While there exists a vast amount of other theoretical threats to mobile devices, this section presents an overview of some of the more practical issues in terms of attacks, threats and vulnerabilities that affect mobile devices. These include, physical device authentication attacks on lost or stolen devices, web based threats such as social engineering and drive-by download attacks.

A presentation of an exhaustive analysis of every possible threat for mobile devices is beyond the scope of this research. The examples presented however do provide a representation of the threats introduced into organizations by allowing mobile devices to access sensitive business information.

3.3. Conclusion

The trends of malicious software that have plagued traditional desktop PC’s for many years have also emerged as a threat on smartphone and tablet PC’s. Similarly, the techniques of distribution and exploitation for mobile devices are also similar to those on traditional PC’s. Mobile malware is distributed without the knowledge of the user and typically runs silently in the background to allow remote unauthorized access to device communications and locally stored information. This modus operandi has developed because malware developers are now driven mostly by financial gain and rather than cause damage to devices as the term ‘malicious’ is suggestive of, instead malware is used to secretly gain access to information.

Furthermore, authentication attacks on lost or stolen devices as well as browser-based and social engineering attacks are some of the additional techniques used by attackers to exploit vulnerabilities in mobile operating systems. The reality is that smartphones and tablet PC's present viable attack vectors for gaining access to organizational networks and their attached endpoint systems or for gaining access to confidential information that might be stored locally on the devices themselves. Before organizations are able to make any decisions related to security policies around mobile devices, it is essential to have a comprehensive understanding of these threats so that the benefits of mobile device use for business can be weighed up against the risks to confidentially, availability and integrity of organizational data.

Chapter 4 – Related Research

This chapter provides reference to research undertaken by both academic as well as industry analysts which are related to the security aspects of BYOD within organizations. The analysis of previous works serves the purpose of understanding the opinions of other authors to extract key concepts for the purpose of creating the questionnaire and is also crucial to ensuring that previous studies are not replicated.

4.1. Shadow IT

Silic and Back [91], use the term ”Shadow IT” to describe the concept of using personal technology for work. The authors refer to “Shadow IT” as the phenomena that “…represents all hardware, software, or any other solutions used by employees inside of the organizational ecosystem which have not received any formal IT department approval”. The difference with this definition to the one provided for BYOD, is that this statement is not limited to mobile devices only, but rather any technology that users would prefer to use without obtaining prior support to do so by the organizational IT Department. BYOD therefore falls under this concept as a sub-category of a much broader topic. The definitions of ‘Shadow IT’ and the ‘Consumerization of IT’ (discussed in Section 1.1) are very much similar and indicate some overlap.

Silic and Back used a combination of literature review, case study and interviews to conduct their research and classify Shadow IT “as an insider threat which is caused by the human factor of an organisation...(i.e. employee) who installs non-approved software without having any malicious intentions”. Unsurprisingly, many of their findings also relate to mobile devices. When asked about trends, one of the respondents stated, “with the arrival of smartphones…we are clearly heading to a mobile Shadow IT”. Concerning risks, one of the interviewees noted that the “biggest threat represents unknown, unverified software that, often, is infected with malware and as such is introduced into the organizational system”. Furthermore, relating to unverified software, another interviewee mentioned that the “…complexity lies in the fact that not only do we have to monitor PCs, but also all devices allowed by Bring You Own Device (BYOD) – which is not a simple task”

[91]. Further findings suggested that countermeasures in the form of technical controls such as network monitoring or operating system domain policy controls that disallowed users from installing software were easy to implement, but also easily circumvented by users who had the technical know-how to do so.

The research concludes that "…employees extensively use Shadow IT software that leverages their productivity and enables faster and better collaboration and communication" and that "…IT risks are greatly increased in the Shadow IT context". The researchers also suggest that "…restriction is a valid countermeasure, but not a solution to Shadow IT challenges that can become opportunities for the entire organisational ecosystem". These findings and suggestions relate strongly to BYOD which may compound endpoint security but also suggest that consumer driven technology, such as mobile devices in many ways provides too many benefits to be completely disallowed from organizational use. In respect of this, a suggestion was made by the authors that educating users with regards to the accompanied risks of the use of such technology would be a better approach.

4.2. Key Factors for BYOD Management - Network Device Visibility and User Awareness

In a journal article, the author Mansfield-Devine [92], conducted an interview with the Certified Technology Officer (CTO) of Bradford Networks, which specialize in Network Access Control (NAC), a technique used to monitor and authorize which devices connect to customer networks. The company also has extensive experience with higher education institutions in the United States. Bradford networks experience in higher education has allowed them to develop a ten step strategy for dealing with BYOD.

The process entails:

1. Determine the mobile device platforms your organisations will allow = Acceptable, Safe Devices;

2. Determine the Operating System versions allowed = secure Mobile Operating System versions;
3. Determine which applications are required and which are not permitted = Mobile Security, Configuration;
4. Determine what groups of employees will be allowed to use these devices = Mobile Device Policies by user;
5. Determine what network access will be assigned based on who, what, where and when;
6. Educate your employees before they buy mobile devices = Mobile Policy Communication;
7. Inventory authorised and unauthorised users = Trusted versus Untrusted mobile users;
8. Inventory authorised and unauthorised devices = Trusted versus Untrusted mobile devices;
9. Controlled network access based on risk posture = Provision network access (NAC);
10. Continuous vulnerability assessment and remediation = enhance other solutions.

An opinion which was emphasised in the interview was that organizations need to start with network visibility. Organizations first need to understand which devices are being used throughout the organization and why they are being used. Once this is learned, the related policies can be developed around that. Another key opinion was that understanding the needs for organizational device use was very important. For this reason, user education and awareness was critical to the success of any BYOD strategy. An opinion echoed from the Silic and Back [91] research.

4.3. Organizational Security Practices Around BYOD Adoption

BYOD surveys in South African organizations are particularly scarce but one such survey has recently been piloted by network infrastructure company Cisco Systems. The questionnaire was conducted during June and July 2014 with future South African business leaders aged between 19 and 35 [93]. The detail of the criteria for the respondents' statuses as "future business leaders" was not shared. The results nonetheless found that 63 percent of South African employees were allowed to use their own devices to access company networks, this accounts for just under two-thirds. The survey also revealed that just under half, 44 percent of South African companies either did not have a BYOD strategy or the employees were not aware of their respective institutions strategy to manage the use of personal devices for work related purposes.

In 2012 Juniper Networks conducted a global survey of mobile device users and IT decision makers to benchmark trust in mobile technologies. 89 percent of business users that participated in the survey claimed that they used their smartphones or tablet PC's to access critical business resources [94]. The survey also revealed that 41 percent of these users used their personal mobile devices for business use without company permission or support. Furthermore, 32 percent of the IT professionals who took the survey expressed concern about employees introducing malware into company networks and 41 percent were concerned about security breaches due to stolen devices. These results show that users almost unanimously indicated that they used their mobile devices for work related purposes and that a fairly large portion of IT professionals felt that this introduced security related concerns such as data loss through malware or physical loss of devices.

4.3.1. Mobile Device Security Policy Implementation

In 2013, Kaspersky Lab conducted the third of its global survey of IT professionals from small, medium and large companies [95]. The survey attempted to discover the key security issues in global corporate IT infrastructure. In this broadly scoped information security study, when asked about the status of their security policies for mobile devices, only 14 percent of the organizations had fully implemented such a policy, 41 percent had policies related to mobile devices that were not fully implemented yet and 32 percent had not established any such policy yet, but were intending to do so. 13 percent of the surveyed companies had no intention of introducing such a policy in their institutions at all. These findings suggest that only a small percentage of the surveyed institutions have fully implemented policies for organizational mobile device use. More alarming were the institutions that had no intention of implementing any mobile device related policy at all. A fair interpretation could be that these institutions are hereby effectively condoning the use of any device onto their organizational network without any intention of control. A policy that completely prohibits mobile device use is safer than having no policy at all. A better strategy would be to recognize the need for policies that either allow or disallow mobile device use or place restrictions on what sort of data is allowed onto the devices.

The Kaspersky survey asked respondents about specific security incidents relating to mobile devices. Alarmingly, 95 percent of the respondents reported that within the past twelve months, at least one mobile device related security incident had been reported by their company. Leaks of corporate data, where mobile devices had some involvement, were reported by 38 percent of the respondents, whilst 33 percent of these cases were linked to the loss or theft of mobile phones. According to 22 percent of the respondents, compromised smartphones also allowed access to other corporate devices. An important difference in this study from the Juniper 2012 survey, was that instead of respondent concerns over data loss, actual incident data was linked to business data loss from mobile devices by more than a third of the respondents. A worrying statistic was that compromised smartphones were leveraged to conduct further attacks on other company devices. This technique is often used with desktop computers that have been infected with remote access trojans (RAT) [96], which allow an attacker control of remote computers to carry out further attacks inside organizational networks.

In 2012, the SANS Institute, which specializes in information security training, conducted two international surveys across various industries to determine the policies and practices that organizations have put in place to minimize the emerging threats around mobile devices. The initial survey which had more than 500 respondents indicated that 61 percent of the organizations allowed personal devices to connect to sensitive network resources and only 9 percent were completely aware of what those device platforms were and which information sources they were accessing. Moreover, 58 percent had no policies for securing these personally-owned mobile devices [97], an alarmingly high figure. In the second survey which was conducted later in 2012 [98], 97 percent of the respondents felt that the criticality of incorporating a mobile security policy into their organizational security and compliance framework was high, indicating that almost all the respondents agreed on this. The survey also found that only 38 percent of the respondents did not have an official policy that addressed BYOD, which is surprising given the unanimous agreement by respondents that such a policy is important. This percentage was nonetheless an improvement over the initial survey where 58 percent reported not having a BYOD policy at all.

A study by Doherty *et al.* [99] examined the composition of the more commonly used, Acceptable Use Policy (AUP) from sixty-five higher education institutions in various countries, which shows the extensive use of this as a control by universities. Their research shows that usage guidelines, information security and access management are some of the more prominently covered themes in university AUP's. However, because of the equally strong emphasis on policy violations and sanctions, the research concluded that instead of proactively promoting desirable security behaviours through user education and guidelines, the primary role of the AUP is that it is being used as a mechanism for dealing with unacceptable user behaviour. Along this premise, an AUP alone is not sufficient to promote secure mobile device usage practices showing the need for specific information security policies.

4.3.2. Implemented Mobile Device Security Controls

Respondents in the SANS survey were also asked which practices their organizations had implemented for protection against malware on mobile devices of which more than 50 percent cited user education as the most commonly implemented control.

With regards to technical controls, organizations are using a variety of systems to control access to information on mobile devices. These range from Virtual Private Networking (VPN), Segregated or Limited networks, Data Encryption, Network Access Control (NAC) and other more traditional controls such as Network Firewalls and Authentication. These strategies have all successfully been implemented as security controls on traditional computing platforms and are now being adapted for protection with mobile computing. Mobile Device Management (MDM), Mobile Application Management (MAM) and Data Sandboxing have appeared as recent strategies for establishing control with mobile computing technologies.

None of these technical controls should be considered a single solution to maintaining the security of organizational mobile device use. Instead a combination or 'layered defense' approach would be a more intelligent strategy to maintaining the security of enterprise data that is stored or accessed by mobile devices.

4.4. User Awareness to Mobile Device Threats

The use of mobile devices for business purposes presents several benefits as well as threats for both device users and their respective organizations. Given the knowledge of these threats, it is worthwhile to determine user security behaviour as well as awareness levels in relation to mobile device threats. There is a growing realization that users are the "…weak link in the chain" [99] with regards to the security of corporate information. The following section discusses academic studies related to the awareness levels of user security behaviours on mobile device platforms.

4.4.1. User Trust in Mobile Applications

As previously discussed, current mobile computing platforms such as smartphones and tablet PC's primarily use centralized software repositories to distribute mobile applications to users. A particular concern around these repositories are that application vetting techniques are not standard practice amongst platform vendors, which has allowed cyber criminals to use this weakness as an attack vector in the less strict application repositories and an increasing number of malicious applications have been discovered in these mobile software repositories.

To determine the security awareness of smartphone users who make use of these application repositories, Mylonas *et al.* [81] surveyed smartphone users by means of structured interviews. The research found that 76 percent of the respondents were of the opinion that applications downloaded from official repositories are secure. This number shows a significant trust level of mobile applications. The evidence previously presented opposes this, and suggests that smartphone security awareness programs are necessary. The researchers also found that users were unaware of the existence or lack thereof, of application testing techniques within official repositories. Specifically, 54.6 percent of users were unaware that mobile application repositories tested application submissions for malicious behaviour, proving that users trust the repository irrespective of the fact that they do not know that application testing takes place. Furthermore, smartphone platforms prompt users with security permission messages at installation time or when requesting access to a resource. The study found that the percentage of users who always inspect these security messages is 38.6 percent.

These findings show that users blindly trust applications which are installed onto their smartphones through official application repositories or are unaware of the dangers of data leakage through malware in the form of trojan applications which are today commonly found on popular mobile application repositories.

4.4.2. Security Controls Adopted by Users

Researchers Mylonas *et al.* [81] also found that in terms of built-in mobile device controls such as device PIN, pattern or password locks, two-thirds of the respondents made use of this security control on their devices, while other built-in controls such as encryption, remote data wipe and remote device location were only adopted by a small percentage of the sample population and that more than a quarter of these respondents did not use any of these physical controls at all. While this study did not specifically survey mobile users who make use of their devices for business use, organizations want to ensure that if BYOD is allowed in their institutions, that all users should be using these basic security controls such as device PIN or password locks.

With regards to third-party mobile security software such as mobile anti-virus, Mylonas *et al.* also reported that less than a quarter of the respondents used this security control on their devices, while 85.8 percent reported use of such software on their personal computers, showing a disparity in user attitude toward mobile security. These findings again substantiate the claim that awareness of threats in mobile device use needs attention. However, as stated by Allam *et al.* [100] "…awareness programs, even if applied, gradually fade into the daily rush of operations from the day they are completed", which emphasizes the need for organizational security policies that enforce these technical controls. Conversely, if security controls are enforced through organizational policy without user awareness programs, users may not understand the need for the controls and refuse policy compliance.

Given that the devices are easily lost or stolen because of device size and that mobile malware has recently seen a substantial growth, these findings suggests a surprisingly relaxed attitude amongst a substantial percentage of users for both physical as well as security related controls. Users want to use new technologies to accomplish their work related tasks and believe that security is not their responsibility, hoping that their companies, service providers or device vendors will seamlessly build security into their interactions [101]. For this reason, user education plays an important role in ensuring secure mobile device use.

4.5. Conclusion

The need for organizational network visibility as well as user awareness is strongly recommended as critical strategies for managing the additional complexity and security risks introduced by BYOD. Organizations however need to first understand the employee business needs for organizational use of personal mobile devices as there are advantages in their organizational use. Conversely, user education would assist users in understanding the organizational risks such as data leakage effected by using personal devices for work related purposes which would thereby increase the likelihood of user policy compliance.

With regards to BYOD adoption, most organizations globally are allowing BYOD and also allowing employees to access critical business resources with their personal mobile devices. Many employees have reported doing so even without special permission from their employers. A strong indication of why employees are doing so without explicitly requesting permission first, is because most organizations have not implemented strategies such as security policies for dealing with BYOD. In South Africa, the situation is for the most part the same. This is worrying because of the extensively reported increase in mobile malware in application repositories, user trust in mobile device software repositories and lack of use of basic device security controls.

Academic research in terms of organizational security concerns around BYOD adoption are rare and even less so when narrowed down to adoption in universities. The examination of the findings of related research however, were useful for determining the status trends, challenges, advantages and risks to organizations brought on by the concept of BYOD. The organizational risks can be managed by the implementation of several technical and administrative controls, but not before a policy is established. These strategies need to be applied as a collective to form a secure mobile device strategy.

Chapter 5 – Research Design

Due to the emergent and compelling nature of BYOD and mobile computing technologies in general, an exploratory mixed-method design approach was used in this study. As stated by Stebbins [102] "…research in any field begins with curiosity". Similarly, Bhattacherjee [103] supports this by stating that, "…exploratory research is often conducted in new areas of inquiry, where the goals of the research are: (1) to scope out the magnitude or extent of a particular phenomenon, problem, or behaviour, (2) to generate some initial ideas (or "hunches") about that phenomenon, or (3) to test the feasibility of undertaking a more extensive study regarding that phenomenon." Furthermore, Johnson and Onwuegbuzie contend that [104], "…both quantitative and qualitative research are important and useful" and that "…the goal of mixed methods research is not to replace either of these approaches but rather to draw from the strengths and minimize the weaknesses of both in single research studies and across studies".

5.1. Methodology

For the reasons above, a mixed-method approach was chosen as the most appropriate method for the study, with the intention of answering the primary research question:

> Are South African universities adopting BYOD and are they aware of the information security concerns introduced into their organizations by allowing this practice? If so, which strategies if any, are being used to minimize these concerns?

Having worked in a South African university environment for a number of years, the researcher made prior observations of the recent trend of co-workers and students increasingly using their personal mobile devices for both business as well as educational purposes. However, with BYOD being a fairly recently recognized phenomenon, only a limited body of academic research exists around the topics related to the security concerns introduced by the use of personally-owned mobile devices for organizations. It was therefore decided that an exploratory study approach would be better suited to discover the BYOD security concerns in organizational settings such as universities.

An extensive literature review was used as the initial data collection procedure to obtain qualitative information regarding the reasons for the sudden interest of using personal mobile devices for work related purposes. Initial searches in academic resources did not reveal many directly related studies such as surveys around the topic within organizational settings. For this reason other closely related technical studies were sought to collect information regarding the security concerns related to BYOD.

Broad searches were done on multiple academic databases to determine the scope of available literature and related academic research on the primary focus areas of Information Security, mobile devices and Bring-Your-Own-Device. A secondary focus area was that of BYOD within South African universities. To determine the keywords and phrases to be used within the searches, websites that focus on Information Security related topics such as InfoSec Island[8], the SANS (Sysadmin, Audit, Networking and Security) Institute[9] as well as others were consulted. The following keywords and phrases were developed:

Bring your own device; BYOD; BYOD advantages; BYOD disadvantages; BYOD higher education; BYOD information security; BYOD organizations; BYOD policies; BYOD risks; BYOD security; BYOD security survey; BYOD university; mobile device; mobile device higher education; mobile device information security; mobile device organizations; mobile device policies; mobile device security; mobile device survey; mobile device threats; mobile device university; mobile device management; mobile malware; mobile security survey; smartphone malware; smartphone security; smartphone threats; university security policy and various combinations of these.

These keywords were used on the Rhodes University library databases such as the ACM Digital Library, CiteSeer, Google Scholar and Science Direct to uncover full-text academic papers on the listed focus areas. When searches on these databases yielded minimal results, searches through the

[8] http://www.infosecisland.com/

[9] https://www.sans.org/

common Google[10] search engine were also performed. Each of the literary works were evaluated for their relevance toward the primary focus areas while keeping in mind that studies related to a higher education environment context would be the foremost consideration. Thereafter studies which related to enterprise or organizational environments were also deemed appropriate.

Analysis of studies related to the information security benefits and risks associated with mobile device use in organizations, was used to address the five research sub-questions (See Section 1.5) from the available literature. As seen in Table 5.1, Table 5.2, Table 5.3, Table 5.4 and Table 5.5, which were developed from the literature summaries in Appendix A, various findings and limitations within the literature survey were discovered. These limitations were then used to determine the objectives of the questionnaire which would ultimately yield the necessary information to make a valuable contribution to academic literature. It must be noted that consultation of both academic and industry-related research was used to achieve the literature survey findings. While the literature provided answers to these secondary questions across a generalized organizational context, research related specifically to the current information security concerns around BYOD adoption within universities were largely non-existent. The literature hereby formed part of the initial qualitative data collection procedure which assisted in determining which questions would be needed for the survey.

Cohen, Manion and Morrison [105] state that "…surveys gather data at a particular point in time with the intention of describing the nature of existing conditions, or identifying standards against which existing conditions can be compared, or determining the relationships that exist between specific events". For this reason it was felt that the most appropriate means of collecting data would be through a survey of South African universities with the objective of discovering that which was not available in literature. Analysis of the survey responses would form the primary portion of the quantitative research.

[10] www.google.com

The following tables show the relationships between the each of the five research sub-questions, the findings related to these within the literature, the limitations of these findings, which were then used in determining the objectives that the questionnaire sets out to achieve.

Table 5.1 – Research sub-question 1

#	Research Question	Findings from literature	Finding limitations	Questionnaire Objectives
1	Do universities have sensitive data that is worth protecting? What security risks are universities faced with and do personally-owned mobile devices increase this risk?	Universities store sensitive data such as: - Personally Identifiable Information; - Research information; - Financial records etc. Leakage of such information has resulted in financial losses and reputational damage for several universities. Mobile devices, if allowed to store such sensitive data, increases the likelihood of information security risks and data leakage due to their potential for theft/loss as well as lack of organizational device control.	The available reports of data loss in universities are by institutions in in the United States. The incidents were caused by both network breach as well as theft of traditional endpoint devices, such as desktop computers that stored sensitive information. Such reports from South African universities are unavailable.	Are South African universities proactively maintaining the security of their sensitive data? Are they addressing the additional risks introduced by personally-owned mobile devices by restricting their access to internal, sensitive and restricted data?

Table 5.2 – Research sub-question 2

#	Research Question	Findings from literature	Finding limitations	Questionnaire Objectives
2	What is BYOD? Define the concept and explore the sudden interest of employee's using personal mobile devices for work related purposes.	Advancements in Internet wireless connectivity such as WiFi 802.11 and 3G networks and their associated improvements on data transfer speeds allow mobile device users continuous access to information from any location. This combined with hardware and software device advancements have assisted Smartphone and Tablet PC's to become useful portable computing devices. While initially designed as personal consumer devices because of their evolution from feature phones, Smartphone usability as computing devices have been realized by employees who want to make use of this functionality to access work-related information, a concept defined as BYOD. This mobile computing functionality has led to widespread global proliferation of Smartphone and Tablet PC users and therefore increases the probability of employees using them to access sensitive work-related information.	Reports of BYOD pervasiveness throughout all industries is very apparent, however their use within South African universities for work or academic purposes are not available.	Are personally-owned smartphones and tablet PC's being used for work related and educational purposes in South African universities? If so, how pervasive is this usage?

Table 5.3 – Research sub-question 3

#	Research Question	Findings from literature	Finding limitations	Questionnaire Objectives
3	What are the current acceptance levels of BYOD within organizations and does this compare to the acceptance levels within South African higher education institutions?	Various industry related surveys provide an indication that mobile device adoption is evident in different industries globally, with employees using their devices to access work related information without first obtaining permission from their employer. Investigating academic literature, and online reports, evidence of mobile device adoption within universities is also apparent with students making use of the advantages of mobile computing options as data collections tools for conducting academic research.	Literature suggests that BYOD adoption is mostly user driven and does not give evidence of acceptance from IT Divisions or Management within organizations, even less so in South African universities who are not likely to not be as eager for organizational use given the associated information security risks that have been previously discussed.	What are the organizational acceptance levels of BYOD specific to South African universities given the Information Security risks? Are the respective institutional IT Divisions allowing BYOD use?

Table 5.4 – Research sub-question 4

#	Research Question	Findings from literature	Finding limitations	Questionnaire Objectives
4	What security threats to organizational data are introduced by these personally-owned mobile devices?	Mobile malware variants are increasing in numbers in direct correlation with the increase in popularity of respective device platforms. Current mobile malware variants have a variety of propagation techniques but is spread mostly through unmoderated application repositories. Literature provides evidence of mobile malware being used to expose sensitive locally stored data from smartphones to remote servers by devices that are controlled over the network. Other threats such as physical device theft, social engineering as well as browser based vulnerability exploitation have been demonstrated by researchers showing the evolution of cyber-crime methods shifting to mobile devices and in some cases, allowing attackers to gain access to other network attached endpoints.	Literature provides us with abundant evidence of the threats that are introduced by the use of mobile devices. However, not enough examples of organizational data leakage through mobile devices were evident. It was felt that the reason for this was because of the recency of the BYOD phenomenon and similarly felt that universities would also not have enough knowledge of such incidents at their institutions. It was therefore decided that the survey would not specifically ask these questions.	N/A

Table 5.5 – Research sub-question 5

#	Research Question	Findings from literature	Finding limitations	Questionnaire Objectives
5	What does the related research inform us about organizational mobile device adoption in relation to BYOD and which strategies are organizations using to mitigate any associated threats?	Similarities to BYOD were identified in a concept known as Shadow IT, where personal technology is used for work related purposes. The same opinions were cited when compared to BYOD in that it increases productivity while significantly increases the information security risks. Restricting the practice was seen as a countermeasure.	While related research points out the opinion of technical representatives within other industries, it does not indicate what the opinions of University technical staff are in relation BYOD and the information security risks.	What are the opinions of technical representatives at South African universities with regards to the organizational Information Security risks? Are these risks exacerbated by BYOD?
		Network visibility is critical to BYOD management. By determining which device types are being used on organizational networks down to OS and application level, organizations can start building policies around their use. However, organizations need to first understand mobile usage scenarios. Additionally, user awareness is cited as a key factor of having a successful BYOD strategy.	Literature does not provide answers to the different device types that are currently connected to SA University networks.	Do South African universities know which devices staff, students and research associates are using to access critical digital business resources?
		Drawing from various industry-related research studies, many organizational representatives are of the opinion that BYOD policies are very important mitigation strategy for security threats. Despite this, very few organizations globally have fully-implemented such policies at their institutions. A cross-industry South African survey revealed that almost two thirds of employees were allowed to use personal devices on company networks. However, very few SA organizations have BYOD polices or their employees were unaware of any such strategies.	While there are some reports and industry related surveys to report on the lack of BYOD policies, reports specific to higher education institutions were not available	Have South African universities implemented Information Security policies related to mobile devices and BYOD? Are these policies being enforced?

As seen in these tables, from the literature review findings, the following objectives were hereby proposed to guide the development of the questionnaire:

1. Are South African universities proactively maintaining the security of their sensitive data? Are they addressing the additional risks introduced by personally-owned mobile devices by restricting their access to internal, sensitive and restricted data?
2. Are personally-owned smartphones and tablet PC's being used for work related and educational purposes in South African universities? If so, how pervasive is this usage?
3. What are the organizational acceptance levels of BYOD specific to South African universities given the Information Security risks? Are the respective institutional IT Divisions allowing BYOD use?
4. What are the opinions of technical representatives at South African universities with regards to the organizational Information Security risks? Are these risks exacerbated by BYOD?
5. Do South African universities know which devices staff, students and research associates are using to access critical digital business resources?
6. Have South African universities implemented Information Security policies related to mobile devices and BYOD? Are these policies being enforced?

5.2. Sampling – Selection of Respondents

As previously outlined in the thesis introduction, the survey was limited to respondents from South African higher education institutions which fall under the classification of Traditional Universities, Comprehensive Universities as well as Universities of Technology, of which there are currently twenty-three institutions within the country. Furthermore, the study was also limited to university institutions that have a physical campus where students are able to attend lectures and have Internet access from a physical network infrastructure within a localized area. This distinction was made as the research deliberates on organizational mobile device use, which to a large extent is achieved by connecting to campus wireless networks. With this in mind, the University of South Africa (UNISA) was excluded because of the absence of a physical campus, bringing the number of institutions now included in the study to twenty-two.

It was then decided that only a single representative from each institution would be needed based on the survey objectives. These objectives meant that the survey would contain a combination of both technical as well as managerial questions and as such, the selection of respondents were aimed at Systems/Network Administrator's, ICT Manager's, ICT Director's and possibly Security Analysts or Managers of central IT Departments within each of the twenty-two institutions. It was presumed that within South African universities, each institution would have at least one such representative.

5.3. Data Collection Procedure

The decision was made that a targeted online questionnaire would be the most suitable means of collecting the required data and was subsequently prepared using a software based survey tool called LimeSurvey. The details for this choice and implementation thereof are discussed in more detail in Sections 5.4 and 5.5.

The next step was to make contact with the ICT Directors of South African universities to assess their willingness to participate in the study. Personal contact was made with the ICT Director of a local university to: (1) request participation, (2) appoint a suitable representative in line with the requirements previously mentioned and (3) request contact details for ICT Directors of other South African universities. The institution agreed to participate and also offered to make initial contact with other institutions countrywide via an ICT Directors mailing list on behalf of the researcher. This offer was welcomed as it was felt that this would encourage participation from other institutions if the request was sent from a known contact. A participation letter with instructions on who to contact if willing to partake, was then drafted for the aforementioned purpose, to be sent via the ICT Directors mailing list, requesting participation and a suitable representative to be appointed. The participation letter included a declaration of who was undertaking the research, for which purposes (i.e. scholarly purposes), as well as the names of the university, the academic department and the research supervisor. An outline of the purpose of research was also included together with field of study.

The data collection portion of the study involved dealing with human subjects and for this reason ethical clearance first needed to be obtained from the Rhodes University Ethics Committee. An ethical clearance form, together with the participation request letter and a printable copy of the full online survey was submitted to the ethics committee for approval. Shortly thereafter, ethical clearance was obtained.

After obtaining the ethical clearance, contact was made with the previously mentioned ICT Director, who was advised to proceed with forwarding the participation request letter to the ICT Directors mailing list. Ten institutions subsequently responded and assigned an individual staff member from their respective IT Departments to partake in the questionnaire. This was a good initial response rate, indicating willingness to participate, substantiating the relevance of the topic within South African universities.

The survey pre-notification letters and instructions were then sent out to these ten participants. Nine out of ten initial responses were shortly thereafter received. Instructions included the amount of questions in the survey as well as the estimated time that respondents should take to complete the questionnaire. After this initial phase, more survey participants were sought to increase the survey sample size. For each of the ICT Directors that did not respond to the initial mailing list request, personally addressed individual emails were sent requesting participation. From the second round of requests, four additional participants were identified and appointed by their respective institutions. These participants were then contacted and sent instructions on how to complete the survey. The return rate of completed questionnaires was not as quick as the first round of respondents, but after telephonic and email reminders two out of four completed responses were received. This brought the total survey response rate to eleven out of fifteen completed questionnaires. The remaining participants who had not completed the questionnaire were sent a final reminder email, but did not respond. It was decided that further responses would not be attainable and the online questionnaire was closed. Eleven completed questionnaires meant that the sample size was exactly half of the entire population and was therefore considered sufficient for the purposes of exploratory research.

The questionnaire was open for a period of seven months, from July 2013 to January 2014.

5.4. Questionnaire Administration

The intention of the survey was to represent all of the twenty-two targeted South African universities and a self-administered online questionnaire was therefore decided on as the most suitable method of data collection. With the survey hosted online, this allowed the questionnaire to reach the widest possible audience and also eliminate travel costs to all the institutions across the country. This is supported by Wright [106] who compared personal interviews with online questionnaires and state that "…costs for recording equipment, travel, and the telephone can be eliminated. In addition, transcription costs and time can be avoided since online responses are automatically documented". Online surveys also allow researchers to reach many people who have common characteristics over a shorter time period, despite being separated by great physical distances. Such cost and time savings were seen as the major advantages for using an online questionnaire considering the great geographical distances between South African universities. Finally, as stated by Kanuk and Berenson [107] "…questionnaires tend to be more valid than telephone and personal interviews because they allow respondents to check information by verifying their records" and "…because they permit leisurely and thoughtful reply".

Hosted on a custom built Web Server, LimeSurvey[11] was chosen as the preferred questionnaire software tool. The reasons for choosing LimeSurvey were due to the application being open-source, free and allowing for unlimited participants. Additionally, a useful feature available through LimeSurvey was the option giving participants a single use token. The questionnaire was restricted to "invite-only", and single use tokens for each respondent were used as a method for controlling and tracking completed responses.

[11] http://www.limesurvey.org

Requests were emailed to respondents from the survey tool itself and participants were provided with a URL and single use token with which to complete the questionnaire.

5.5. Questionnaire Design

As previously stated, an exploratory approach was determined as the most suitable for the research to be carried out, and an online questionnaire would be used as the data collection tool primarily for the reasons outlined below:

- The BYOD phenomenon has only recently been observed as a worrying occurrence for organizations because of the recent increased usage of smartphone and tablet PC's in work related environments, as such there is very little academic research around organizational security concerns on the topic, even less so in universities. For this reason, there exists very little research to test any grounded hypotheses against for complete quantitative analysis.
- Given the recency of smartphone and tablet PC's for business use, it was felt that not all respondents would be particularly well versed in the knowledge area around the associated security issues and terms. By using an online questionnaire with preconfigured answer options, this would assist less experienced respondents in this regard.

Questionnaires which use closed-ended designs allow researchers to produce quantitative data rapidly, but the richness of potential responses is lower because the possible answers options are set by the researchers not respondents. As stated by Boynton and Greenhalgh [108] "…closed ended items often cause frustration, usually because researchers have not considered all potential responses".

The questionnaire was therefore designed in such a manner that it could be analyzed both quantitatively as well as qualitatively. This was achieved by predominantly using closed questions with preconfigured answer options, using "other" as an option throughout, which also hints at the exploratory nature of the research. Additionally, where appropriate, participants were encouraged to comment and elaborate on their choices in an open ended answer box. Finally, before ending the survey, respondents were asked an open ended question and were asked to share any questions or suggestions regarding the topics that were not represented by the survey. The intention of this being that the written response data would allow for more qualitative detailed analysis of the previous answers. Miller and Dickson [109] are of the view that online qualitative research is an apt method for obtaining respondent data when: (1) the target population is small, (2) the participants have highly specialized skills and (3) when the study relates to high-tech products and services. Conversely, the responses to the closed questions were analyzed quantitatively when participants only selected the preconfigured answer options.

5.5.1. Questionnaire Introduction

Walonick [110] states that a cover letter is an essential part of a survey which allows the researcher with an opportunity to persuade the respondent to complete the survey and that "…to a large degree, the cover letter will affect whether or not the respondent completes the questionnaire". With this in mind, each respondent was presented with an introductory web page when initially starting the questionnaire, which served the purpose of a cover letter.

The introduction page provided participants with an explanation of: (1) the purpose of the questionnaire, that the research was being undertaken for scholarly purposes, (2) the reasons for the research, to gain insight into the security maturity levels relative to BYOD in higher education institutions, (3) participant instructions and benefits, such as who to direct queries to and the incentives for participating and (4) confidentiality and ethics, explaining to all participants that collected data will not be presented in a manner which identifies the respondent or institution in any published reports.

In order to increase respondent response rate, the introduction also informed participants that the questionnaire contained only thirty-eight questions and that any published reports would not contain any identifying information thereby guaranteeing respondent and institutional confidentiality.

5.5.2. Questionnaire Grouping

As discussed, it was felt that not all participants would be familiar with all the related terms and concepts. For this reason, the questions were arranged into logical groups instead of a single set of questions to assist respondents with context by providing overarching categories. Walonick [110] states that "…grouping questions that are similar will make the questionnaire easier to complete, and the respondent will feel more comfortable." The purpose of each category is also briefly described at the beginning of each section to provide further clarity to the respondents.

According to Gillham [111] questionnaires are principally composed of two basic types of questions. The first being 'subject descriptors', such as age, gender or occupational category which describe the people who have taken the questionnaire. The second type of questions are those which provide data on the topic you are studying. The subject descriptors are there to provide relevance to the topic being discussed. The questionnaire was therefore structured in this way, with 'Respondent Profiling' and 'Institutional Profiling' being the preliminary question groups. These two sections contained only questions about factual data and none containing respondent opinions.

Thereafter, the survey was divided into the following question groups based on the questions which were determined by the empirical objectives previously discussed:

- Institutional Policies – This section assesses the institutions' policies on usage of ICT services and will be used to compare these policies on usage specific to BYOD.
- Management, Controls and Opinions – This section assesses the security controls deployed by the institution to enforce the policies related to personally-owned mobile devices.
- Suggestions – This section allows participants to address any specific questions or suggestions that they would like to share that was not represented in the survey.

The question groups were intended to assist participants with question context but also to assist the researcher when analyzing the collected responses.

5.5.3. General Question Considerations

In order to prevent incomplete responses, LimeSurvey was used to configure the majority of the questions as mandatory. This is indicated by the star/asterisk at the end of each question in Appendix B and ensured that the respondents were not able to complete the questionnaire without answering these particular questions. These mandatory questions however always included an “other” or “don’t know” option to allow respondents to opt-out if the question could not be answered to prevent respondent frustration. At the discretion of the researcher, certain sensitive questions and open-ended questions were specifically not made mandatory, to allow participants to skip if not willing to answer.

To further refine the questionnaire by minimizing unnecessary questions, LimeSurvey features were used to configure required conditions for certain questions where necessary. As an example, when asking respondents about the reasons for implementing a mobile device policy, this question would only be presented to respondents who had previously answered that they had implemented such a policy in the first place. For respondents who answered that their institution had not implemented any mobile device policy, the follow up question would become redundant and therefore is skipped and not presented to the respondent at all. If this follow-up question was not skipped and was instead asked to a respondent who had indicated that their institution had no such policy, the question may be deemed nonsensical to the participant. This approach was therefore used to avoid such confusion whenever appropriate.

5.6. Pre-Testing the Survey

According to Iarossi [112]“…the pilot represents the first live test of the instrument, as well as the last step in the finalization of the questions”. In line with this, when the first draft of the survey was completed, a pilot test of the survey instrument was conducted. Three test questionnaires were sent to willing participants who were university employees with technical experience working in South African institutions. This pilot test was done for a number of reasons: (1) to request that respondents provide feedback with regards to difficulty of any questions that need improvement, (2) to observe and estimate the length of time it would take to complete all of the questions and (3) to test the validity and reliability of the survey tool.

From the feedback, it was determined that the survey should take respondents no longer than twenty minutes to complete and that the questions were clear and comprehensible. The pre-test respondents reported that they had not experienced any confusion while answering any of the questions and a decision was made to leave the survey as is for the eleven selected participants.

5.7. Conclusion

In this chapter, it was discussed in detail that an exploratory research design and mixed-method methodology would be used for the research. The participant selection and data collection process was also discussed along with the use of a questionnaire and its design and implementation phases. A copy of the entire survey can be viewed in Appendix B.

Chapter 6 – Questionnaire Results

As discussed in the research design, participation requests were initially sent out via email to IT Directors of various higher education institutions within the South Africa to appoint a single representative from their institutions to complete the questionnaire. A good response rate was achieved, with 11 completed questionnaires out of a possibility of 22 selected South African universities. This resulted in a final response rate of 50 percent.

6.1. Respondent Profiling

The aim of this section in the questionnaire was to obtain demographic data to verify that the selected target group criteria was met. Respondents were asked to indicate their organizational role at their respective institutions, the experience they have accumulated within the ICT field and to confirm that they were employed at a South African higher education institution. Questions 1 to 3 in the online questionnaire was used to obtain this information.

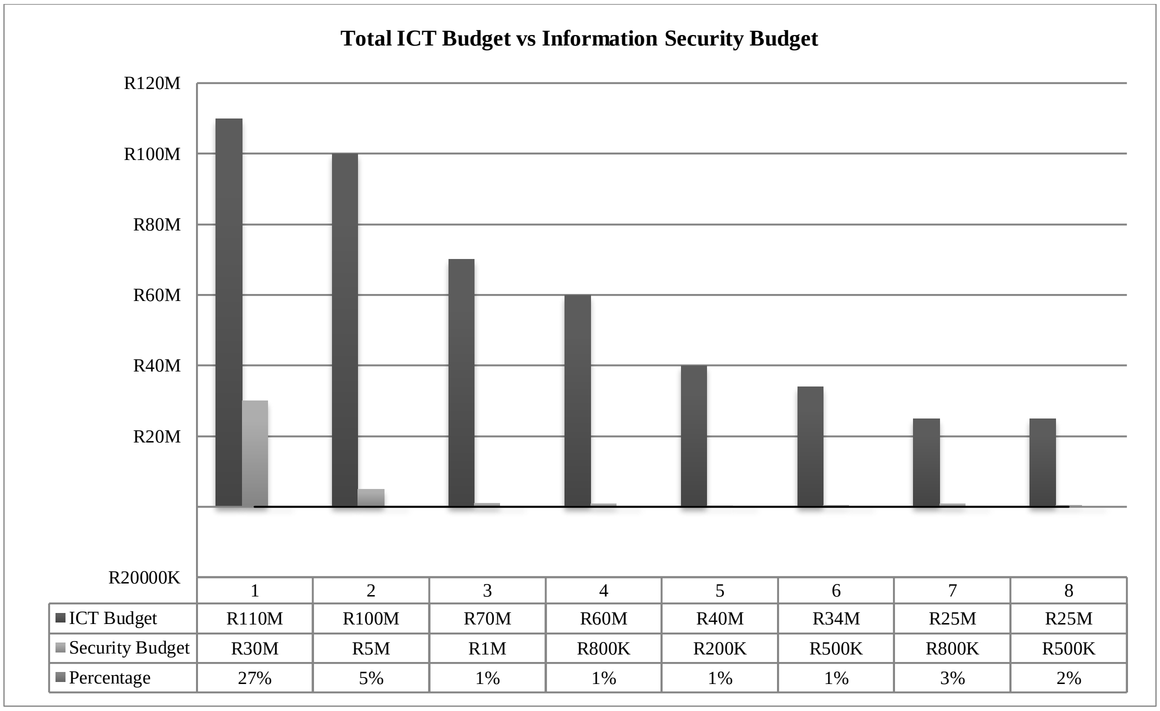
All of the respondents confirmed that they were employed at South African higher education institutions, which was expected as only participants from higher education institutions were initially invited. This question was nevertheless included for the purpose of validation. Of the 11 participants that took part in the survey, 4 were ICT Systems Managers and 2 were ICT Security Services Managers. The remaining 5 respondents were made up of an ICT Director, IT Manager, IT Risk Manager, Operations Infrastructure Manager and ICT Senior Configuration Specialist. All of these positions were relevant to the targeted respondent profile.

With regards to work experience, 8 of the respondents indicated that they had between 10 and 30 years of experience, 2 of the respondents had between 5 and 10 years' experience and a single respondent had less than 5 years' experience in the ICT field. This indicates that the respondents who took part in the survey come from a range of different positions within the ICT field and that at least 72 percent of these people have more than 10 years of experience.

6.2. Institutional Profiling

This section was included to assess the institutional student and staff population size, the ICT budget and security budget, as well as which mobile device strategies the institutions have in place.

6.2.1. ICT Budget



	1	2	3	4	5	6	7	8
■ ICT Budget	R110M	R100M	R70M	R60M	R40M	R34M	R25M	R25M
■ Security Budget	R30M	R5M	R1M	R800K	R200K	R500K	R800K	R500K
■ Percentage	27%	5%	1%	1%	1%	1%	3%	2%

Fig. 6.1 – Total ICT Budget versus Information Security Budget

Respondents were asked in Question 4 what their annual institutional ICT budgets were and immediately asked in a follow up question what their annual institutional spend on information security related services and products were. The resulting data was used to determine what percentage of the ICT budgets were dedicated to information security. While not compulsory, the response rate was good, with 8 out of 11 respondents revealing their institutional budgetary information.

It was found that two of the larger institutions allocated above R100m annually for their overall ICT budget, with the maximum being R110m and the minimum being R25m, as seen in Fig. 6.1.

When this is contrasted with the ICT Security expenditure, all but one of the institutions in the sample allocated 5 percent or less toward security services. This single outlier, indicated that 27 percent of their ICT budget, is allocated to information security services. If the mean is calculated from these percentages, it is found that on average, South African universities allocate 5.1 percent of their annual ICT budget toward Security. If the outlier institution is excluded from the dataset, then the mean percentage of security spend amongst the other universities becomes 2 percent. According to Kirk [113] as espoused by Gartner, globally businesses spend an average of 5 percent of their total IT budget on security, which demonstrates that this proportion of expenditure within South African universities is not abnormally low when compared to other organizations. However, this does not necessarily mean that the global average is acceptable, but because the practice of Information Security is a trade-off between the impact of data loss and the cost of data protection, each individual organization needs to review their budgetary allowances on an individual basis, based on their risk assessments. For this reason, it is almost impossible to suggest an acceptable annual information security budget. The survey results do however indicate that for the majority of South African universities, security services are not high on the expenditure priority list.

6.2.2. Information Security Technical Staff

Respondents were asked in Question 6 to indicate if their respective institutions had a distinctive section or post for information security staff within their IT Departments. The resulting data show that none of the institutions have a dedicated “Information Security” section within their central IT Department.

However, it was found that 5 out of 11 of the institutions have an explicit “Information Security” role within their IT Divisions, making up 45 percent of the survey sample. The remaining 6 respondents indicated that their institutions did not have a specialized information security role at all, making up 55 percent. This demonstrates that there is an almost even split, between whether or not the institutions employed a full time information security post, or whether they had no such post at all with the split being slightly in favour of the latter.

The institutions that did not employ a staff member in this specific role meant that most of the university IT Staff either handled information security responsibilities as a secondary role as part of their regular duties in some way. The unlikely scenario that the institutions were not consciously practicing any information security strategies at all is negated by the fact that all of the respondents indicated that a portion of their ICT budget is dedicated toward information security related expenditure.

6.2.3. Staff and Student Population

To assess the impact of potential data loss, it was necessary to evaluate the population sizes of the institutions. As such respondents were asked to indicate what their staff and student counts were in Questions 7 and 8 respectively. For student counts, the relative survey responses were grouped into four categories, 5000 to 15000 (small sized), 15000 to 25000 (small to medium sized), 25000 to 45000 (medium to large sized) and more than 45000 (large sized).

Arranged from smallest to largest, a single institution reported having a student count of between 5,000 and 15,000 students. Thereafter, 3 institutions in the sample indicated population sizes of 15,000 to 25,000 students, with another 3 indicating their university having between 25,000 and 45,000 students. These were categorized into small to medium sized and medium to large sized institutions respectively. Lastly, 4 respondents indicated that their institutions had more than 45,000 students and thus were categorized into large higher education institutions as seen in Table 6.1. Not surprisingly, the student count of the institutions aligned with the indicated ICT budgets, with larger institutions also generally having larger ICT budgets.Table 6.1, the dataset has been arranged in order of student populations from smallest to largest as this shows the grouping of student number populations in a more effective manner. As the student numbers increase, so too do the staff, which is expected. As discussed earlier in the literature (See Section 2.1.3), the University of Maryland (UMD) reported the data theft of 288,000 current and previous personal records after a discovered data breach. As a result, the institution offered credit protection services for those affected, which became costly because of the amount of people affected. As seen in a 2014 online report, UMD [114] had a student undergraduate enrolment count of 27,056 in 2014 when the incident took place. Many of the South African universities in the survey sample have a similar or even larger student count than UMD and this demonstrates the huge financial impact that such a data breach may cause.

Table 6.1 – University Staff and Student count

Institution Sizes	Institution	Students	Staff
Small	1	5,000 - 15,000	501 - 1,000
Small to Medium	2	15,000 - 25,000	501 - 1,000
	3	15,000 - 25,000	1,001 - 2,500
	4	15,000 - 25,000	2,001 - 5,000
Medium to Large	5	25,000 - 45,000	2,001 - 5,000
	6	25,000 - 45,000	5,000 - 10,000
	7	25,000 - 45,000	5,000 - 10,000
Large	8	More than 45,000	2,001 - 5,000
	9	More than 45,000	2,001 - 5,000
	10	More than 45,000	5,000 - 10,000
	11	More than 45,000	5,000 - 10,000

6.2.4. Institutional Mobile Device Strategy

Respondents were asked if their respective institutions had developed a strategy for the implementation of mobile devices to investigate if the institutions were generally making changes to their ICT Infrastructure and Services, to accommodate the proliferation of mobile device users.

When asked in Question 9 if their institution had implemented any mobile device strategy regardless of device ownership, 6 out of the 11 respondents indicated that they had not yet implemented such a strategy, implying that 55 percent of the surveyed intuitions intended to do so in the near future. 4 out of 11 (36 percent) indicated that they had partially implemented a formal strategy towards mobile devices. One of the respondents that indicated they had a partially implemented mobile device strategy commented that their institution was implementing wireless infrastructure on all of their campuses but that management of devices and security policies have not been implemented. While there may be many reasons for this approach, of which exploring all the possibilities are beyond the scope of this research, it does show a similarity with the assertion by Leavitt that [115] "…wireless service providers have long focused on communications and other services, with security remaining an afterthought". Many organizations lack this recognition of the significance of including security during system development which in turn results in little or no budget allocation for information security strategies. Choobineh *et. al* [116] state that it is a norm to check whether or not the security holes remain unplugged only after a system has been implemented and refer to this as a checklist culture. This checklist approach results in lack of consideration for context and business processes within which the checklists are then applied to.

A single respondent indicated that their institution had no intention of implementing any mobile device strategies. None of the institutions indicated that they had fully implemented a formal strategy towards support and services for mobile devices. Given that the proliferation of mobile devices within business environments is a fairly recent trend, this was anticipated.

The questionnaire followed up this initial question by asking respondents about mobile device strategies, however a contextual change asked the respondent to indicate whether or not their institution had implemented a mobile device strategies specific to user-provisioned devices. 4 out of 11 or 36 percent of the respondents indicated that they had not yet implemented strategies for user provisioned mobile devices, while 5 or 45 percent of the respondents indicated that they had partially implemented such strategies. The 2 remaining respondents were split between having no intention of implementing any strategies specifically for mobile devices and a fully implemented mobile device strategy.

6.3. Institutional Policies

In order to determine the organizational maturity levels of South African universities with regards to BYOD, the respondents were asked various questions about the support trends within their institutions and the related organizational policies that have been implemented to manage the use of personally-owned mobile devices. This section was developed to fulfill the empirical objectives of investigating the acceptance levels and pervasiveness of BYOD use within South African universities. Additionally, it also investigates the empirical objectives which seek to determine which mobile device platforms are prevalent and which of these devices are being used to access business resources.

Lastly, more common information security policy practices were also investigated to determine the organizational security baseline and were compared with policies and usage that are specific to personally-owned mobile devices.

6.3.1. Mobile Devices Widely Supported

To assess the level of support being offered for mobile devices, Question 11 asked respondents if their institution currently allowed Internet capable devices such as smartphones and tablet PC's onto their institutional networks.

The results reveal that the majority of South African universities are supportive of mobile device use. This is evidenced by the fact that 5 out of 11 (45 percent) respondents indicated that their institutions allowed tablets and smartphones onto their network and are changing their network services and online content to be able to actively support such devices. Furthermore, another 5 respondents indicated that their institutions allowed such devices onto the institutional network but were currently offering "network only" access and were not focused on changing their services in support of tablet and smartphone devices. Only a single respondent indicated that his/her institution allowed "network only" access that has been purposefully restricted into certain areas of the institutional network, such as Internet only access.

These results show that the BYOD acceptance levels amongst South African universities are high, with none of the institutions choosing to completely restrict personally-owned mobile device use. An even split amongst the sample occurred between those who were actively changing their services to support BYOD and those who currently only offered access to the institutional network. A concerning finding was that only one of the institutions were restricting network access to limited areas of their institutional network. This is remarkable in that this configuration would be considered one of the safer options in terms of security. From these findings it is possible to deduce that the acceptance levels of amongst South African universities are very high.

6.3.2. Mobile Device Count

To determine the pervasiveness of personally-owned mobile device use within the survey, Question 12 asked respondents to indicate how many personally-owned, Internet-capable mobile devices were currently registered on their institutional networks. To encourage responses as seen in Table 6.2, pre-selected device count ranges were given to respondents instead of just allowing respondents to enter a specific number.

As seen in Table 6.2, 2 of the 11 respondents indicated that their institution had no means to reliably calculate how many personally-owned mobile devices were registered on their institutional network. A single respondent indicated a device count between 100 and 250 personally-owned mobile devices registered on their institutional network. 3 of the 11 respondents indicated a device count range of between 250 and 1000 personally-owned mobile devices and lastly, 5 respondents indicated that their institution had a device count of between 1000 - 5000, personally-owned devices that have been registered on their institutional network.

Table 6.2 – Mobile Device Count

Device Count	**Number of Institutions (n=11)**	%
No way to reliably determine (Unknown)	2	18
0	-	-
n < 0	-	-
11 – 100	-	-
100 – 250	1	9
250 – 1,000	3	27
1,000 – 5,000	5	45
5,000 – 10,000	-	-
n > 10,000	-	-
Sum of Institutions aware of device count	9	82

The information suggests that majority of the survey respondents were able to determine how many personally-owned mobile devices were registered on their networks of which 45 percent of the institutions had a device count within the thousands. These results show the proliferation and pervasiveness of mobile device use within South African universities and is therefore aligned with the findings in literature which suggest that mobile devices are increasingly being used in business environments. This suggests that South African higher education environments are not an exception, as personally-owned mobile devices are being increasingly used in university environments as well.

Additionally, an interesting finding was that only 2 of the institutions had no way to determine how many mobile devices were connected to their networks. This result is positive in that shows that 9 out of the 11 institutions, accounting for 82 percent already have the network visibility referred to by Mansfield-Devine [92] as being a key factor for BYOD management. However, a more desirable result would be to have this finding at 100 percent instead.

6.3.3. Mobile Device Count Increasing

To determine the extent of BYOD proliferation within South African universities, respondents were asked in Question 13 if the amount of personally-owned mobile devices on their networks have increased within the last two years.

Table 6.3 – Device Count Increase

Device Count	Number of Institutions	%
Decreased slightly	-	-
Remained relatively unchanged	-	-
Increased slightly	1	9
Increased significantly (doubled)	5	45
Increased significantly (tripled)	2	18
Increased immensely (more than tripled)	3	27
Don't know	-	-

As evidenced in Table 6.3, none of the institutions indicated that the number of devices have decreased or remained unchanged over the past two years, indicating clearly that the numbers of these devices are growing. A single respondent indicated that mobile devices increased slightly, while the majority of respondents felt that mobile devices increased significantly. When broken down into further detail, 5 of the 11 respondents felt that personally-owned mobile device numbers have at least doubled, 2 respondents felt that the number had tripled and 3 respondents felt that mobile devices numbers have more than tripled. This further validates the premise set forth in the literature that business use of mobile devices is increasing at a rapid rate and illustrates the pervasiveness and current popularity of bringing personally-owned mobile devices onto university networks. It is therefore accurate to deduce that the trend of BYOD has recently increased significantly within South African universities.

Within the literature, it was discussed that the current personally-owned mobile devices are susceptible to similar threats and vulnerabilities as traditional computers as well as additional vulnerabilities that are unique to mobile devices such as the higher probability of loss or theft. As such, given the pervasiveness clearly evident from the responses, it is of important that South African universities implement strategies to mitigate the associated mobile threats.

6.3.4. No Restrictions on Mobile Device Platforms

In Question 14, respondents were given a multiple choice question to select from a list of the current popular mobile device types, as concluded in Section 2.2.2, to determine which of these are allowed onto their institutional networks. This question was asked to determine if institutions were restricting network access to certain device types. Respondents were allowed to choose from Windows Mobile, Google Android, Apple iOS, RIM BlackBerry and Symbian OS as answer options. Additionally, respondents were also asked to indicate if they did not plan to restrict certain device types, automatically indicating that all of the aforementioned mobile devices operating system platforms were supported if this choice was made.

A single respondent, out of the 11 participants, indicated that their institution only allowed RIM BlackBerry devices onto their networks. Another single respondent indicated that all of the mobile operating systems were allowed onto their networks, with the exception of Symbian OS. Out of the remaining respondents, 4 selected all of the multiple choice options, indicating that they allowed all of the current mobile device operating systems onto their networks, while 5 respondents indicated that their institution was not planning to restrict certain device types.

The responses show that only one the institutions represented in the survey have restricted their network access to RIM BlackBerry exclusively and a single institution restricted Symbian devices from their networks but allowed all of the other major platforms. The majority of South African universities however are allowing network access from any of the current mobile operating systems. To be more specific, 36 percent of the institutions allow network access from all of the aforementioned mobile operating systems and 45 percent have no intention of restricting access from any of the devices platforms at all. The latter statistic also automatically infers that all of the current mobile platforms are allowed by these institutions as well as any other platforms that employees and students may want to use in future. As such, the combined percentage of South African universities that allowed all of the current mobile operating systems onto their networks is 81 percent. This again shows that the acceptance levels for the current mobile operating systems are high amongst South African universities. The more concerning statistic however is the 45 percent that that do not plan to restrict certain device types which suggests an open door policy. Allowing absolutely any device onto institutional networks could make BYOD management extremely complex. As discussed in the literature, Bradford Networks [92] suggest that the first step in a BYOD strategy for higher education institutions is to determine which safe and acceptable mobile devices your organisation will allow.

From a usability perspective, it is understandable why the institutions would not plan to restrict access to certain mobile platforms. The nature of university business is centred on research which includes exploration and openness to learning and as such often includes openness to use of the technologies such as the current mobile devices which facilitate such learning. Restricting certain devices would therefore seem counterproductive. A more secure solution would be to evaluate certain device platforms and then combine this with Identity Management (IdM) solutions to restrict less secure device platforms to low risk users only. As an example, it is not uncommon for universities to restrict students to certain, less sensitive areas of the network only, which makes student user accounts low risk. Allowing these low risk users to use any device is not a big concern as students generally do not need access to restricted areas of the network and this would not affect their productivity. However, if university administration staff such as the Director of the Finance department, who is likely to have access to highly sensitive data is allowed to use an insecure mobile platform, the associated physical threats as well as online-based threats discussed in – Technical DiscussionChapter 3, places this sensitive data at a much higher risk.

In conclusion, most universities in South Africa do not restrict certain mobile device platforms and instead seem to have an open door policy. The possibility exists that the surveyed institutions have fully evaluated and tested all of the device types and are therefore content that these platforms meet their security compliance standards. As discussed in Chapter 2 some mobile platforms are more susceptible to threats than others and as such it is surprising that hardly any restrictions are placed on their access. Another plausible scenario is that the institutions do not have any device compliance standards and policies in place and simply allow any device to connect their networks. Discussed in more detail in Section 6.3.6, it is revealed that a large majority of South African universities have not implemented any policies that govern the use of mobile devices which strengthens this theory.

6.3.5. Device Access to Business Resources.

Question 15 presented respondents with a rating scale to determine how confident South African universities were at knowing which devices were accessing their business resources. These ratings scales, as represented in Table 6.4, were grouped into varying degrees of confidence and were represented to respondents in percentages as follows:

- Not Confident - 0 percent
- Vaguely Confident – between 0 and 40 percent
- Fairly Confident – between 40 and 75 percent
- Extremely Confident – between 75 and 99 percent
- Completely Confident – 100 percent

The results show that only 2 out of the 11 respondents felt that they were extremely confident in knowing which devices were being used to access business resources while the rest of the institutions were split between fairly confident and vaguely confident by 45 and 36 percent respectively. What is noteworthy, is that none of the respondents were 100 percent confident in knowing which devices were accessing their business resources.

While these results are more positive than negative, a more desirable result would be to have all of the institutions at the "Extremely Confident" level. Only 18 percent are currently at this maturity level. Previous studies which ask a similar question within South African universities do not exist. This would have allowed the research to expand on whether or not the respondents were more or less confident before the BYOD trend which amplified the use of personally-owned mobile devices. As stated by Disterer and Kleiner [50] when discussing the approach of using Mobile Device Management (MDM), "…Companies should have the ability, especially when data is stored locally, to erase all company data from a device when access to data should no longer be granted (e.g. loss or theft of device, end of employment)." As in this case, having the ability to remotely wipe business information from user devices is impossible without knowing which devices have access to this data first.

Table 6.4 – Knowledge of Device Access to Business Resources

Confidence Rating	No. of Institutions (n=11)	%
Completely (100%)	-	-
Extremely (75 – 99%)	2	18
Fairly (40% - 75%)	5	45
Vaguely (0% - 40%)	4	36
Not Confident (0%)	-	-

In conclusion, this information demonstrates that the majority of South African higher education institutions are not yet highly confident in knowing which device types are accessing their critical business resources.

6.3.6. Lack of Policy Implementation

Questions 16, 17 and 18 asked respondents about the level of implementation of policies at their institutions to assess if their respective ICT Departments have used this as a method of control within South African universities. For each policy that the respondents were questioned about, they were asked to indicate if the policy has been fully implemented, partially implemented or not implemented at all, with questionnaire guidelines to the implication of each. 'Fully implemented' implies that the policy has been published throughout the institution and only minor changes are necessary whenever the policy is revised. ‘Partially implemented’ implies that the policy is still in its infancy and more rules are constantly being added. ‘No Policy’ which is self-explanatory implies that the institution has not implemented the policy at all.

Acceptable Use Policy

As seen in Fig. 6.2, a pie chart is used to demonstrate the policy coverage within the institutions. With regards to the Acceptable Use Policy (AUP), 6 out of the 11 respondents or 54 percent indicated that their institution had fully implemented this, while 4 or 36 percent had partially implemented an AUP. A single institution had not implemented an AUP at all.

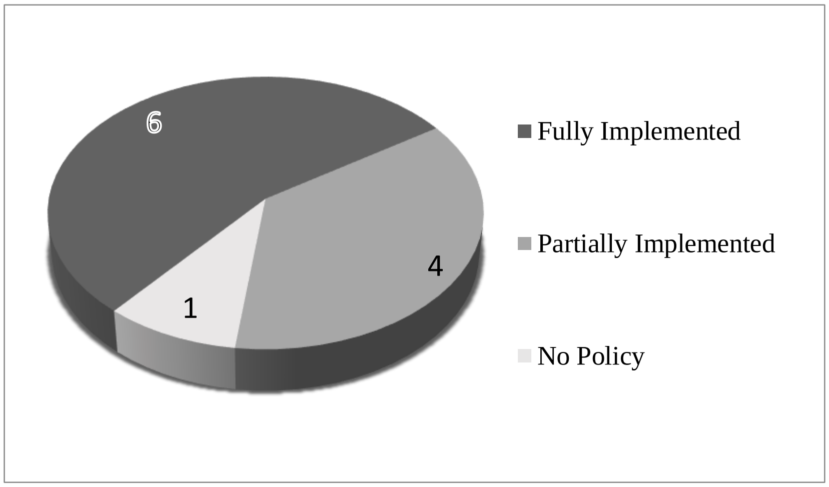


Fig. 6.2 – Acceptable Use Policy coverage

As discussed earlier in Chapter 4, the formulation and application of an AUP is seen as an important mechanism for minimizing the occurrence of inappropriate behaviour on computer-based information resources [99]. Most AUP’s are used to facilitate security of core production systems such as servers from internal misuse and a good policy should also include every other network object such as routers, switches and device endpoints. Young and Aitel [117] state that without this policy in place, organizations may be liable for any illicit activities caused by its employees. As such, it is a positive result to see that with the exception of a single institution, 10 out of 11 or 91 percent of the survey sample have this important policy in place. While the AUP is not specifically a mobile device policy, it still serves as an important baseline policy for organizations to have.

Information Security Policy

As seen in Fig. 6.3, the institutional information security policies within the survey sample are not as widely covered as the AUP's. Whereas 6 of the institutions had a fully implemented AUP, 5 institutions or 45 percent had fully implemented information security policies. Additionally, 3 of the institutions or 27 percent have a partially implemented information security policy, which is better than having no policy at all. As such, the combined count for institutions that have an information security policy is 73 percent. Less positively, the remaining 3 institutions did not have this policy at all.

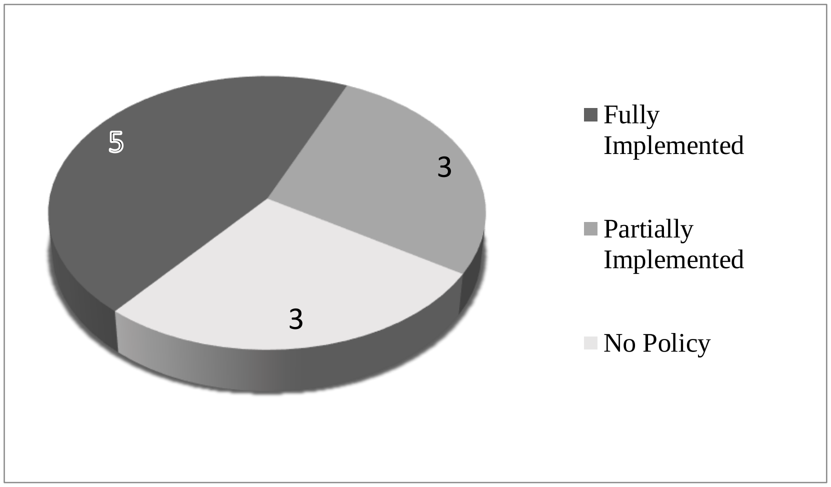


Fig. 6.3 – Information Security Policy coverage

University core education and research activities are reliant on the confidentiality, availability and integrity of computer based information and have been so for a number of years. It is therefore surprising that less than half of the institutions have fully implemented this policy. Additionally, all of the respondents in the sample indicated that their institutions have thousands of students, which infers that large amounts of personal as well as research data is stored on their information systems. For this reason, security policies should be a top priority and ideally, all of the institutions should have an information security policy. However, the reason for this lack in policy is likely due to the lack of dedicated information security staff as discovered earlier (Section 6.2.2). This data was cross-referenced to check if this premise is true and it was found that each of the 3 institutions which did not have an information security policy, also did not have a specific information security officer or role within their institutions.

BYOD Policy

According to Schneider [118] general-purpose security policies have attracted the most attention, but the application-dependent and special-purpose security policies are becoming increasingly important". Policies that govern the use of personally-owned mobile devices fall into this special purpose category. As seen in Fig. 6.4, BYOD policies are even less widely covered than both the AUP and information security policies within the survey sample. Given the recent surge of the BYOD trend, this result was somewhat expected.

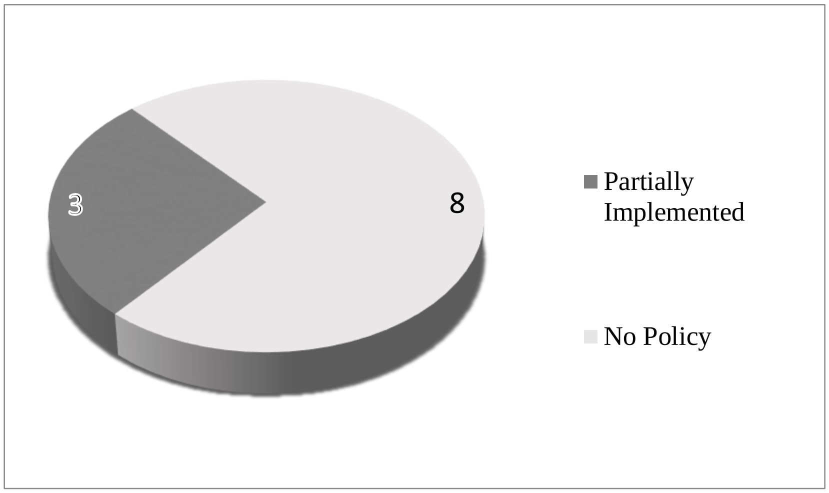


Fig. 6.4 – BYOD Policy coverage

Whereas with the AUP and information security policies, which were implemented by 90 percent and 73 percent of the institutions respectively, when asked if their institutions had a published policy for personally-owned mobile devices, only 3 respondents or 27 percent indicated that their institutions had a partially-implemented policy. The remaining 8 institutions indicated that they did not have such a policy at all. As such, none of the institutions had a fully-implemented BYOD policy.

These statistics reveal that only a very small percentage of the institutions in the sample have proactively implemented BYOD policies. Having no mobile device policies means that institutions have no specific rules regarding mobile devices. For this reason, it is not surprising that the majority of the respondents indicated that certain device types were not being restricted.

It should also be mentioned that although current mobile devices have brought the BYOD trend under more scrutiny, the concept itself is not entirely new. Users have used their personal devices such as laptops or flash memory sticks on company owned devices and networks in the past. As such, policies that govern personally-owned devices should at least have been partially implemented by a majority of the institutions, whereas in reality, only 3 institutions have done so. In conclusion, South African HE institutions are still in the developing phase with regards to policies for both information security as well as BYOD.

6.3.7. Policy Compliance

According to Vance *et al.* [119], it has been estimated that more than half of all Information Systems security breaches are caused by employee failure to comply with information security procedures. For information security policies to be effective, these policies have to be strictly enforced. This argument is strengthened by Von Solms [120] who declares that (1) “not realizing that a corporate information security policy is absolutely essential” and; (2) “not realizing that information security compliance enforcement and monitoring is absolutely essential” are two of the deadly sins of information security management. As such, to assess the institutional rigorousness toward policy enforcement, respondents were asked if the consequences of non-compliance of ICT policies at their institutions were clearly communicated and enforced.

The results show that only 2 or 18 percent of the institutions felt that their policies were being strictly enforced. 4 of the respondents or 36 percent indicated that their policies were only partially enforced whilst the remaining 5 or 45 percent indicated that their policies were not strongly enforced. The results suggests that the majority of the institutions that took part in the survey believed that their institutional policies are not strongly enforced.

These responses shows that SA HE institutional IT Departments do not appear to be greatly concerned about policy compliance. Another likely scenario is that the IT Departments do not have the necessary support from other stakeholders within their institutions. For policies to be successful, they need to be thoroughly published, comprehensible and strongly enforced. The enforcement usually requires the IT Division to work in conjunction with Top-Level management and other departments such as Human Resources as these sections will be required to pass judgment among staff or students within the institution. The role of central IT is an enabler of technology and should not be relied on to make decisions in disciplinary action. If HR and Top management are not involved in the decisions around ICT policies, enforcement becomes very difficult.

6.3.8. BYOD policies are Considered Critical

To investigate the respondent's opinions with regards to the necessity of BYOD policies. Question 22 asked respondents to indicate the importance of the need to incorporate BYOD policies into their overall Security and Compliance frameworks. A rating scale of 'Unimportant', 'Important' and 'Critical' were given as answer options as well as a 'don't know' option to allow respondents to opt out if they were unsure.

The responses were particularly interesting when placed into context with the BYOD policy implementation results in Section 6.3.6. While it was found that only 27 percent of the institutions have only partially implemented BYOD policies, all of the respondents felt that incorporating BYOD policies into their security frameworks were either important or critical. Discussed in more detail, 5 of the respondents or 45 percent indicated that BYOD policies were important, while the remaining 6 respondents or 55 percent indicated that it was critical. This indicates that all of the respondents felt that policies for personally-owned devices were indeed needed by their institutions and in fact more than half of the respondents indicated that this need was critical.

To conclude, all of the respondents have at least realized a need for BYOD policies even if these have not been implemented as yet.

6.3.9. Summary - Institutional Policies

With regards to acceptance levels of BYOD, the survey results found that the majority of South African universities are allowing the use of personally-owned mobile devices onto their networks. Additionally, the number of devices being used have increased rapidly over a short time period, which is in line with global industry, as is widely discussed in literature.

With this in mind, all of the respondents were of the opinion that implementing policies for personally-owned mobile devices were greatly important for their institutions. Which is why it is surprising that only a very small percentage of these institutions had only partially implemented such a policy, while being aware of and allowing for the rapid increase of mobile devices on their institutional networks.

Additionally, the majority of respondents were split between being fairly confident and vaguely confident of which devices were accessing their business resources, which is worrying but also a common side-effect due to the unmanaged nature of personally-owned mobile devices. This is an indication of the need for stricter control and device management to offer protection against data loss and the security concerns associated with mobile devices.

Finally, it was found that of the security policies that were implemented, few of the institutions were strictly enforcing these policies while the majority of the institutions felt that policies were not being strongly enforced at all. Even the best policies and procedures will have little value if they are not followed. Choobineh et al. [116] state that not enforcing the consequences of committing a policy violation is analogous to police never patrolling the highway for speeders. When an organization does not periodically audit their operational use, a false sense of security around its intellectual properties may be developed, leaving valuable information assets vulnerable and subject to compromise. Furthermore, policies that govern BYOD use were only partially implemented by a small number of South African universities in the survey sample.

6.4. Respondent Opinions on Mobile Device Risks

This section seeks to fulfill the empirical objective of finding out if respondents felt that organizational security risks within universities are exacerbated by BYOD. As such, respondents were asked their opinions with regards to the data security risks which are created by the use of personally-owned mobile devices within South African universities.

6.4.1. BYOD Risk versus Advantages

Question 30 was used to determine respondent opinions with regards to the risks versus the advantages that are introduced into institutional networks by the BYOD trend. Respondents were asked to indicate if BYOD:

- Introduces more negative risks than positives and advantages; or
- Introduces more positives and advantages than negative risks; or
- Introduces a similar balance of both risks and advantages.

Out of the 11 respondents, 7 were of the opinion that BYOD introduces a similar balance of both risks and advantages. Thereafter an even split of 2 each between BYOD introduces ‘more risks than advantages’ and ‘more advantages than risks’ were answered by the remaining 4 respondents. These results therefore are inconclusive that any one opinion is shared over the other, however they do show that the respondents believe that the trend does have advantages, even though they are aware of and acknowledge that there are additional risks which are introduced by mobile devices as none of the respondents opted to use the “other” or “do not know” answers.

6.4.2. Mobile Devices Increase Risk of Data Loss

For further analysis on the opinions of the additional risks introduced by BYOD, Question 32 asked respondents if they felt that the risk of data loss was increased by allowing Smartphone and Tablet PC’s to access business resources in their environments.

A rating scale was given to respondents which asked them to indicate if:

- The risk of data loss and security breaches is significantly increased over and above traditional risks;

- The risk of data loss and security breaches is only slightly increased over and above traditional risks

- The risk of data loss and security breaches over and above traditional risks remains the same and is not at all increased.

The findings were that and the 6 out of 11 respondents or 55 percent felt that the risk of data loss is significantly increased by allowing Smartphone and Tablet PC's access to business network resources. 5 out of 11 participants or 45 percent felt that the risk of data loss is only slightly increased. This results in an almost even split in opinion, in favour of risks being significantly increased. However, what is more indicative of the feeling of increased risk is that none of the respondents felt that the risk to business resources remains the same or are not increased by Smartphone and Tablet PC's.

While the opinion therefore holds true that Smartphone and Tablet PC's introduce a higher risk factor for data loss, only a few of the institutions have implemented BYOD policies as evidenced in Section 6.3. The reasons for the lack of policy while being aware of the risks and still supporting the devices in this case reveal that usability is being placed ahead of security on the scale of importance.

6.4.3. Smartphone and Tablet OS Security versus Desktop OS Security

To further explore the question of increased risk, question 31 asked respondents what their opinions were when comparing the security features of current Smartphone and Tablet operating systems versus those of traditional Desktop and Laptop operating systems. The responses indicated that 5 respondents or 45 percent felt that traditional desktop operating systems offer better security features than mobile operating systems. Opposing this opinion, only a single respondent was of the opinion that mobile operating systems offer better security features than desktop operating systems. The remaining 5 respondents remained indifferent and were of the opinion that both mobile devices and traditional desktops are equally secure.

Furthermore, some of the respondents that felt that traditional desktops offered better security features elaborated on the reasons for this response in the provided comment section. One of the notable comments were, "*We have more control of the desktop environment".* The interpretation of which is likely because of the fact that existing desktop management controls have already matured within traditional enterprise environments which previously consisted mostly of Microsoft Windows operating systems. Furthermore, these Windows PC's were physically connected to corporate Local Area Networks. Mobile devices now expand this access wirelessly to any location from any of the various versions of Android, iOS, BlackBerry and Windows Phone operating systems, making management and control exceedingly complicated.

The noteworthy finding was that only a single respondent felt that mobile devices offered better security than traditional desktop operating systems. From the resulting responses of the survey sample, it is therefore reasonable to suggest that from the combined responses that traditional desktop operating systems are considered more secure than mobile device operating systems.

6.4.4. Mobile Operating System Threat Comparison

Respondents were also asked if, in their opinion, certain mobile device platforms introduced a significantly higher amount of security threats than others. 5 out of 11 respondents answered "No" and 6 answered "Yes". While this information does not really suggest much as the number of respondents are relatively evenly matched in their opposing response. A follow-up question was however asked to the six respondents who had answered "Yes" to elaborate on why they had this reasoning. They were asked to indicate which of the current mobile operating systems would introduce the highest percentage of security threats into the institutional network.

As seen in Table 6.5 – Mobile OS Threat Comparison, the eye-catching result was that it was unanimously agreed by all of the 6 respondents that Google's Android operating system would bring the highest percentage of threats to the institutional network. These 6 respondents were then cross-referenced with the results of Section 6.3.4 which asked which mobile operating systems were allowed onto institutional networks. It was found that all of the respondents had previously indicated that the Android mobile operating system was allowed onto their networks despite them having a sense of increased threat.

Table 6.5 – Mobile OS Threat Comparison

Operating System	Number of Institutions (n=6)	%
Google Android	6	100
Apple iOS	2	33
RIM BlackBerry	2	33
Microsoft Windows Phone	1	17
Symbian	-	-
Other	-	-

This result was anticipated and a follow up question was therefore asked to these 6 respondents to indicate if the devices which they selected as having a high threat rating would be restricted from accessing critical business resources. Unanimously, all of these respondents indicated that such restrictions would not be enforced because this would be opposed to a true BYOD strategy.

To expand on this discussion, Mills [121] posed a similar question to security experts regarding Apple Mac (OSX) versus PC (Windows) in a small informal online web survey. One of the experts commented that "…they are both mature operating systems from the security point of view, and as good as each other. But, crucially, it's not about the operating system that is being run on the computer, it's the fleshy human sitting in front of it". To elaborate on this, both Apple Mac users and Windows users are equally likely to install a malicious browser plugin to watch a bogus online video and would even be willing to enter their user authentication credentials and elevate user privileges to do so. As such, social engineering is the threat that puts all computer users at risk irrespective of the operating system that is used. However, within the same informal survey, the majority of experts seem to agree that while neither of the operating systems are inherently more or less secure than the other, many were of the opinion that Apple Mac OS X is definitely the safer operating system, simply because malware writers are targeting Windows which has a larger user base and as such, the larger attack surface. A similar opinion can be related to the mobile device operating systems.

In conclusion, this data suggests that there is an almost even split of 45 and 55 percent in favour of respondents' opinion that certain mobile operating systems introduce more network threats than, those that do not. There is truth in both arguments but it is certainly truer that currently, the Android operating system would introduce more device based vulnerabilities into organizational networks than other current mobile operating systems. It was established in the literature review that malware writers are focusing their efforts on the Android operating system for various reasons, with the principal one being the larger user base.

6.4.5. Mobile Device Anti Malware

As an added layer of security on traditional desktop computers, anti-virus client software is considered almost standard in current workplace environments with large networks and endpoint devices. The subject is however controversial in that many security professionals justly argue that anti-virus is only partially successful at detecting known samples of malicious software. For this reason, Question 34 asked survey respondents if they felt that mobile device anti-virus was necessary if smartphones and tablets were allowed access to business resources.

A single respondent selected the 'don't know' answer option, while another respondent was of the opinion that mobile anti-virus or anti-malware is not needed. Conversely 8 or 73 percent of the respondents felt that mobile anti-virus software was just as important as it is on desktop computers. The conclusion from these results are that the majority of respondents feel that mobile anti-virus is indeed a necessary security control.

6.4.6. Summary - Opinions on Mobile Device Risks

The results in this section reveal that the institutional technical representatives that took part in this survey show a valid awareness of the risks associated with the use of personally-owned mobile devices. The majority have a shared opinion that BYOD does indeed increase the risk of data loss within their institutions. There is also an indication that the majority of the respondents felt that Smartphone and Tablet PC operating systems are less secure than traditional desktop operating systems. Finally, the majority of the respondents also felt that mobile anti-virus is necessary before allowing access to business resources on personally-owned mobile devices.

Chapter 7 – Recommendations

This chapter is included to provide a brief guideline on the steps and strategies that universities can use to manage the security risks associated with business use of personally-owned mobile devices.

7.1. Develop a Mobile Device Security Policy

The National Institute of Standards and Technology (NIST) recently developed a Special Publication report entitled "*Guidelines for Managing the Security of Mobile Devices in the Enterprise*" [122] which offers organizations good recommendations about developing a complete strategy for securing both corporate-owned as well as personally-owed mobile devices in large organizations. The recommendations offer a rigorous five-phase model, which NIST has identified as a "Security for the Enterprise Mobile Device Solution Life Cycle". The five phases are discussed as being: (1) Initiation; (2) Development; (3) Implementation; (4) Operations and Maintenance and; (5) Disposal.

Within this first initiation phase, which involves developing a "…vision for how mobile device solutions support the mission of the organization" one of the first steps which are detailed is developing a mobile device security policy. The policy details which organizational resources may be accessed by mobile devices, the degree of access, and the various mobile platforms which are allowed to access these business resources. NIST recommends that the policy should be included in the overall security strategy of the organization. What the NIST document does not specify, but indirectly implies, is that before the mobile security policy can specify "…which types of the organization's resources may be accessed via mobile devices", the organization first needs to have a data classification policy in place. Data classification views institutional data as digital assets and groups this data based on the level of sensitivity and value to the organization. Examples of the types of data assets in universities were discussed in Chapter 2 of the literature review. Once the data classification policy has been established, this will not only aid in development of the mobile device policy, but also various other security policies and controls that the organization needs to implement in future.

As discussed in the survey results, only 27 percent of South African university institutions that took part in the survey had partially-implemented mobile device policies. However, even though the organizations had not yet established the policies, the majority of respondents viewed the BYOD policy as critical. This is in line with NIST's view, as it is listed as the very first part of the Enterprise Mobile Device life-cycle.

7.1.1. Policy Content

While there are many important components to include in the organizational mobile device policy and each organization should make its own decision on what these are, a very important recommendation for universities is to stipulate the different access levels allowed between user groups such as academic staff, administrative staff, research associates and students. This element should originally be stipulated in the organizations overall information security policy and is essential for universities because it is largely the differentiating factor between corporate business environments and university business environments. Students do not need access to sensitive information stored by university registrar or finance divisions and therefore should not be granted permissions to these resources. This should be communicated and enforced through policy. For example, students could be allowed restricted Internet-only access from their devices, whereas administrative staff, depending on their identity could be allowed to access more sensitive digital information from their mobile devices. As stated by Steiner [123], "…with BYOD, it is more important than ever to control which individuals have access rights to the network from their personal devices".

It is evident that having both a general information security policy as well as mobile device specific policy is essential as these documents would contain references to the other. In other words, it is worthwhile to keep in mind that the mobile device policy should be consistent with and supplement the information security policy for non-mobile systems. According to Souppaya [122]. It is in the mobile device policy where the organization establishes the rules such as, employee responsibilities, which devices and associated software are permitted or restricted, required configurations for devices, explanation of technical support and consent to certain practices such as allowing the organization to remotely wipe the device if it is lost or stolen to prevent data leakage. If the organization feels that mobile devices increase their data leakage risks by too great a degree, the policy should communicate that personally-owned mobile devices are completely restricted, however it must be kept in mind that having a policy such as this that is unreasonably strict will foster user backlash and non-compliance. It is important to always keep in mind while developing the policy that anytime anywhere access is what makes BYOD so appealing in the first place [123]. Conversely, having no policy at all means the organization has no standing in legal arguments with regards to loss of data resulting from the loss of a mobile device. Additionally, any organization that does not have a policy has no means of enforcing any form of desired control. It is therefore important to establish a policy which clearly explains all the desired practices and regulations.

7.1.2. Policy Enforcement

Once the policy has been developed and finalized, it is important to remember to enforce the penalties of non-compliance on a regular basis. Similar to maintaining that motorists require a driver’s license when driving a vehicle on public roads, the policy will only be of value if the consequences of not adhering to policy are enforced. For example, in a scenario where a user removes the device PIN configuration on his/her mobile devices. Consider soft penalties like banning the device from network use for a reasonable time period. If the user actually had any productivity benefits from using their personal mobile device for work purposes, they would hereby feel restricted without its use. The user will soon learn the importance of adhering to the policy.

All of these policy restrictions will however need centrally managed technical mechanisms to assist with the enforcement. Software products such as Mobile Device Management, Mobile Application Management and Network Access control become useful which are discussed further in Section 7.3.

7.2. Threat Modelling

Following on with the NIST model, the second ‘development’ stage considers the necessary technical characteristics needed to ensure success of the policy. Throughout this development phase, an important strategy to aid institutions while developing the mobile device policy is to develop a threat model based on the threats to the digital assets that are exposed by the use of mobile devices within the organization. The degree of risk and mitigation strategies are then developed based on the identified threats.

The concept of threat modelling is not a new one. People instinctively conduct risk assessments and threat models on a day-to-day basis. People think about the crime and threats in the different neighborhoods in which they live. As an example, someone living on a farm in a rural settlement with less few tangible assets is more likely to leave their home unlocked than someone living in an urban environment with expensive furniture. In fact, the latter would probably want to increase the security of their home by adding security gates onto doors, windows and all other entry points and even include alarm systems with monitoring. However, people are not always good at accurately considering risk, sometimes grounding their assessment on their emotions. Hulme [124] offers a good analogy by comparing people’s fear of shark attacks versus accidents at home or higher fear levels of an airplane crash than a car accident when the statistics prove that the latter is far more likely to happen [125].

The same goes for threat modelling within organizations as it is important to initially understand what each of the threats are. When applied to mobile devices, it is important to precisely determine what each of the threats are, in specific cases, instead of trying to protect against absolutely everything. Thereafter, as the threat model portfolio matures, more and more threats should be added. In Chapter 3, many of the threats faced by mobile devices were discussed in depth and as such, only a summary of these are included below to provide some examples of how threat models for mobile devices can be developed.

7.2.1. Threat Modelling in Practice

Threat modelling should begin with organizations asking themselves what the mobile device threats are and what the effects are of the specific threat. Some examples of how this is accomplished are provided in Table 7.1, Table 7.2, and Table 7.3. A table for the threats should be created together with description; occurrence likelihood rating; risks; and the mitigation strategies for each:

Threat Model 1:

Table 7.1 – Threat Model (Device Loss or theft)

Threat	Mobile Device loss or theft
Description	Due to the smaller form factor, these devices are very portable. While this is one of the primary advantages of mobile devices, this portability also increases the probability of misplacing the device in public areas.
Likelihood of Occurrence	Medium-High
Description of Risk	Attacker gains physical access to the mobile device. Sensitive information such as business email's or locally stored business documents are now disclosed to unauthorized persons. Additionally, because of the smaller keyboard screen, saved credentials on mobile device applications and configuration profiles are commonplace. If the device VPN client has been configured with a VPN profile and saved authentication credentials, this could allow an attacker access to the organizations internal network via the device which could potentially allow for remote access to sensitive intranet-only information and other attached network devices.
Mitigation Strategies	Staff mobile devices should be protected by a passcode or PIN when the device goes into standby or is locked. Devices should be configured to be auto-locked after a reasonable time period (e.g. 5 minutes) This should be enforced by a combination of policy and technical controls such as Mobile Device Management (MDM). On Android devices, pattern locks should not be allowed as they are susceptible to easily exploitable smudge attacks, only PIN or passwords are configurable options.
	Both personal data as well as organizational data becomes combined on local storage of user-provisioned mobile devices. As such, remote wipe and local storage encryption functionality is not practical in the sense that user personal data may be wiped in error. It is therefore more sensible to prohibit local storage of *sensitive* business data on personally-owned mobile devices altogether. This requires data classification policies to first be established. Employees working with sensitive data should be informed that they need to familiarize themselves with data which is classified as restricted. Such data is only accessible via VPN and only available online, with local copies being prohibited. User education and awareness is a key strategy in getting users to understand this strategy.

Physical loss or theft of a device represents the most obvious risk of data loss that is introduced to mobile device users and their organizations. With the devices storing more sensitive data, it is important that they are adequately secured using basic protection strategies such as PIN or passcode locks to prevent disclosure of such information when discovered. As seen in Table 7.1 the likelihood of occurrence is rated as “Medium-High”. This is because of the size of mobile devices and hence this should be identified as a more serious risk. It is therefore important that the appropriate mitigation strategies are applied.

Threat Model 2:

Table 7.2 – Threat Model (Browser-Based attacks)

Threat	Browser-Based Attacks
Description	Mobile devices are always on and almost always connected to the Internet, either via the organizational wireless network or cellular data connection and because of this there remains a permanent risk of browser-based attacks occurrences. Attackers can use commonly known software and application vulnerabilities to remotely access information stored or transmitted by the mobile device.
Likelihood of Occurrence	Medium
Description of Risk	Similar to desktop operating systems, without regular updates to mobile operating systems and their applications, attackers could remotely gain unauthorized access to sensitive information through a combination of software engineering and exploiting known operating system vulnerabilities.
Mitigation Strategies	Advise staff to keep their devices up to date with the latest software via user education and awareness programs. To encourage participation, inform users that this will increase the security on their devices and thereby protect both their personal as well as organizational data.
	Network Access Control (NAC) should be used to query endpoint devices for baseline security information. If devices have outdated, vulnerable operating systems, these should be given limited (Internet only) network access until the OS is updated. N.B. It should be noted that this technology is not fool proof and advanced users would be able to spoof their devices network information. This solution however does provide a degree of protection for the majority of users and thereby mitigates a large proportion of the aforementioned threat.

As with desktop operating systems, mobile operating systems also suffer from software vulnerabilities that are being exploitable by attackers by using browser-based attacks such as drive-by downloads. These vulnerabilities are usually updated by platform vendors after discovery and for this reason, it is important to maintain updates for mobile devices in the same way that desktop operating systems and their respective applications should always be updated to the latest versions. This mitigation strategy should be encouraged and implemented as discussed in Table 7.2

Threat Model 3:

Table 7.3 – Threat Model (Mobile Malware)

Threat	Mobile Malware
Description	Mobile Malware is usually found in the form of trojanized applications on untrusted 3rd party application repositories which are allowed by default on certain mobile device platforms. If use of these platforms are allowed, mitigation strategies need to be established to minimize the threat of mobile malware on these devices. With more mobile malware samples being discovered daily, the risk of mobile devices being infected with malicious code is steadily increasing.
Likelihood of Occurrence	Medium
Description of Risk	Mobile Malware could allow remote data leakage on devices, remote device control and thereby allow sensitive organizational information to be compromised by an attacker.
Mitigation Strategies	Stipulate via policy that mobile anti-virus is compulsory on user devices if they are allowed to connect to business networks. Enterprise mobile anti-virus solutions will be used to minimize known threats.
	User training and education: Inform users about Social Engineering dangers and following SMS or social media URL links. Just as users are advised of these dangers on traditional desktop computers, so too do they need to be aware of similar risks on mobile devices. Inform users that mobile malware is mostly found on untrusted 3rd-party application repositories. Educate users about the dangers of installing applications from unknown repositories and advise them that this behavior is both dangerous to them as well as the organization. Where possible, prohibit users from using 3rd-party application repositories completely.
	Majority of mobile malware is found on untrusted 3rd-party application repositories. Educate users about the dangers of installing applications from unknown repositories and advise them that this conduct is both dangerous to them as well as the organization. Where possible, prohibit users from using 3rd-party application repositories completely.
	Do not allow jailbroken or rooted devices to connect to university wireless networks. Also disallow users from escalating application installation privileges on Android devices that allow users to install applications from unknown app sources (By Default, Android configures this setting to be off). Network Access Control (NAC) is a mature technology that can be used to achieve this objective by denying network access to non-compliant devices.

Currently, most mobile malware attacks are targeted at consumer applications that have direct transactional value, hence the risk from this threat for enterprises is currently not yet highly significant. However, as discussed in the literature (See Chapter 3), there is evidence of mobile malware that displays remote control characteristics, this is reason enough to implement mitigation strategies to protect against the threat as seen in Table 7.3.

These are some of the more common threats that exist and how to manage them through basic threat modelling. The list is by no means exhaustive and the idea would be to periodically update list of mobile device threats.

7.3. Technical Controls

The aforementioned threat modelling examples bring forward technical controls that a mobile policy needs for successful implementation. Thus, the ‘implementation’ phase involves identifying and making use of centralized technical controls that supplement the implementation. A variety of such technical controls exist and should be used in combination to achieve the mitigation strategies identified in the threat modelling process.

It is also important that the technical controls that are implemented are able to integrate with common enterprise infrastructure such as IdM systems and Lightweight Directory Access Protocol (LDAP) user directories. This will ensure that the organization can delegate mobile devices access permissions accordingly. This also means that the structure of such directories have to be correctly configured in the first place.

What is important is to first identify the technical needs in the previously mentioned ‘initiation’ and ‘development’ phases, as these are critical in determining the needs of technical controls such as MDM, MAM and MCM.

Examples of these existing controls and how they are used are summarized below:

7.3.1. Mobile Device Management

MDM suites allow for the software-based network enforcement of security policies, applications, configurations and even inventorying of mobile operating systems. Apple’s ‘Profile Manager’ [126] is one such solution that offers a high level of granular control for iOS devices and only requires an OS X Server license making it an inexpensive option. The drawback is that Apple’s MDM only has configuration options for Apple devices. For this reason, it is better to invest in a third-party cross platform solution that has the necessary management features to manage all of the current mobile operating systems. Companies like Zenprise and AirWatch offer some of the more popular cross-platform MDM’s currently on the market. The idea behind MDM products are not necessarily only to provide security for mobile devices, but rather control, of which lack thereof is greatly the reason for initial security concern with personally-owned mobile devices as discovered by the results of the survey.

7.3.2. Mobile Application Management

MAM is similar to MDM but differs in that it is a centralized software suite that only focuses on provisioning, control, update and monitoring of the applications found on mobile devices. This is often considered a less intrusive approach to MDM and allows organizations to track and scan for rogue applications on user devices, while also being able to provision company specific developed applications to users. The benefit of MAM is that it allows the organization to specify which applications should be used to connect to business resources so that any data that traverses to and from devices are delivered in a secure contained application that has been pre-approved by the organization [127].

7.3.3. Mobile Content Management

MCM is a security focused mobile management suite that focuses on secure document management through authentication and authorization. MCM is considered the least intrusive of technical controls in that it does not attempt to control the device or applications, but instead delivers a single application to the users mobile device which then has access to a document repository [127]. It is then possible to limit access between read-only, change/edit and full document access. While this solution might seem like the most obvious solution to BYOD in that it does not alter user devices in any way and merely secures the data which is the most important asset, it should be kept in mind that MCM is unable to protect an organization from threats such as a stolen user mobile device which is configured with a VPN client and saved credentials and not having a device PIN as described in the threat modelling scenario earlier.

7.3.4. Network Access Control

Access control is a commonly used mechanism in computer security that allows network administrators to make use of Access Control List's (ACLs) to filter access to certain resources based on specified rules. In the general sense, ACLs are usually applied to users. However when these ACLs are applied to computer endpoints, intermediate routers, proxies and any other network hosts, in order to limit access to network specific resources, this practice is then referred to as Network Access control (NAC) [128]. NAC vendors such as Bradford Networks [92] have started adapting their products to apply filters for mobile devices because of the recent popularity of BYOD trends. The benefit of NAC is that it allows network administrators to establish filters in line with the mobile device policies that scan and block unqualified devices from connecting to the network. As an example, if the NAC system detects a jailbroken or rooted device connecting to the wireless network, such a device can be automatically blocked or placed into a quarantined (Internet only) network.

7.4. User Education

Once the policies, threat models and necessary controls have been established, the final step is to ensure that users are aware of the risks associated with the business use of personal mobile devices. As seen in the threat modelling process, certain threats such as Social Engineering are impossible to mitigate with technical strategies. Employees must be educated on each specific threat identified during threat modelling that specifically relates to the users. Again, it not necessary to have such educational sessions with the entire organization including students and all staff, but rather to top-level management that have access to sensitive materials. User awareness can be performed in many ways, by having documented procedural guidelines on an organizational website or sent out in a monthly institutional newsletter.

What is important to remember is that user education should be designed in a manner that informs the user of their responsibilities, which is set out in the aforementioned policy and also to inform them of the risks for both themselves and the organization. If the education materials are made to feel as though they have the user interest at heart, users will be more willing to comply and follow the laid out guidelines.

The main goal in user training is to "…raise awareness of the risks and issues regarding the use of mobile devices, teaching, not only the rules of the BYOD scheme within the company but also best practices to stay safe when away from work". [58]

7.5. Conclusion

Once the BYOD policies, threat models, controls and user education strategies have been established, it is important to periodically perform assessments to confirm that each of the processes and phases are being performed effectively and to determine how they can be improved. This falls in line with the 'Operations and Maintenance' phases as suggested by NIST's model. Similarly, regular upgrades of any of implemented solutions need to be regularly performed as with normal infrastructure maintenance.

This chapter has provided a comprehensive summary of recommended strategies and practices universities and other institutions could follow to help secure their organizations from the data loss threats associated with the use of personally-owned mobile devices. If these steps are followed, they provide concrete procedural guidelines that will ultimately save the organization from the financial and reputational damages associated with the loss of sensitive business and private data.

Chapter 8 – Conclusion and Future Work

The work presented in this study makes an essential contribution to information security literature as it was discovered during the early phases of the project that academic papers containing topics that covered the organizational security concerns around the use of mobile devices were largely absent.

It is also believed that the majority of the original research objectives which were discussed in the introductory chapters have been achieved. This chapter hereby provides a summary of the research that has been carried out with a focus on how these objectives were accomplished. To conclude, the identification of future work that may facilitate other projects is then also deliberated on.

8.1. Research Objectives

This debate specifically focused on the concerns within university environments where the institutional culture promotes open sharing of information instead of protecting it. For geographical reasons, it was felt that the research would be better suited to be carried out with South African institutions for the ease of data collection. A number of goals were discussed in Chapter 1 with the idea of deliberating on the information security concerns brought about by the use of personally-owned mobile devices in work related environments. These original research objectives are summarized below:

- To contribute to academic literature with regards to the security concerns around enterprise BYOD adoption and hereby incite further research.

- To provide guidance with regards to the security considerations when implementing a BYOD strategy within universities and similar organizations.

To achieve these objectives, a primary research question was proposed:

> Are South African universities adopting BYOD and are they aware of the information security concerns introduced into their organizations by allowing this practice? If so, which strategies if any, are being used to minimize these concerns?

This primary research question was further expanded into five research sub-questions in order to aid in achieving the research objectives.

The findings of sub-questions one to three, implicitly address the first part of the primary research question "Are South African universities adopting BYOD and are they aware of the information security concerns introduced into their organizations by allowing this practice?..." and similarly, questions four and five address the second part of the primary research question "…which strategies if any, are being used to minimize these concerns?". As such if these sub-questions are addressed this implies that the primary question is automatically addressed. For this reason the sub-questions and how they were dealt with are reflected on below.

1. "*Do universities have sensitive data that is worth protecting and what risks are universities faced with?*", was addressed in the literature in Chapter 2 (Section 2.1) where the various data loss concerns were discussed by use of real world examples of data breaches and their resulting impact for the affected institutions. Thereafter, the use of an online targeted questionnaire provided insight to the second part, "do personally-owned mobile devices increase this risk?"

2. "*What is BYOD? Define the concept and explore the sudden interest of employee's using personal mobile devices for work related purposes?"* was addressed in Chapter 2 (Section 2.2) of the literature review, where a synthesis of literature from various sources were used to define the concept of BYOD and discover the reasons for the current trend. This delivered a crucial understanding of the history of the change in the computing landscape toward the current mobile computing environment. This also gives an understanding of the productivity advantages that organizations get by allowing BYOD.

3. "*What are the current acceptance levels of BYOD within organizations and does this compare to the acceptance levels within South African higher education institutions?*" sub-question was addressed in two parts. First, in Chapter 2 (Section 2.3), current practices within organizations were discovered through literature which reference real world examples and reports. It was discovered that many organizations are both directly and indirectly accepting BYOD into their environments due to the push from users. Similar results were then found in the practices of South African universities through the evidence discovered in the questionnaire. High acceptance levels of BYOD were noticeable, along with the recognition from questionnaire participants of the related security threats.

4. "*What security threats to organizational data are introduced by these personally-owned mobile devices?*" was addressed in Chapter 3 (Section 3.1 and Section 3.2) and primarily drew upon existing literature to discuss the increasing levels of mobile malware and mobile device related threats respectively. A discussion of how these issues may perpetuate information security risks for organizations were reflected on.

5. The final sub-question "*What does the related research inform us about organizational mobile device adoption in relation to BYOD and which strategies are organizations using to mitigate any associated threats?*" was addressed by reflecting upon similar studies in Chapter 4 which suggests that BYOD is inevitable for most organizations because of the many advantages it offers both the institution as well as the employees. However, BYOD has many disadvantages such as data loss concerns and ultimately increases the attack surface for any organization. The survey was composed and found that the pervasiveness of mobile device adoption in South African universities compared to other organizations. Additionally, because related academic research was not found in literature the survey sought to determine which mitigation strategies South African universities were using. The results suggest that many of the common controls have not been implemented. For this reason, recommendations for the implementation of a secure BYOD policy was suggested in Chapter 7. A threat modelling procedure was also suggested to aid in creating the policy.

Finally examples of mitigation strategies such as technical controls and user awareness were discussed.

By addressing the five sub-questions, the primary research question was thus addressed and in so doing, the original research objectives were achieved.

8.2. Future Work

Throughout this project, several elements were discovered that could deliberated on into their own projects.

During the design of the questionnaire, it was realized that because of the small population size of the targeted group, there would be great difficulty in achieving a large enough sample size for quantitative analysis only. As such it was decided that the questions would be designed to allow for the collection of both qualitative and quantitative information. The questions allowed respondents the option of commenting on their answers or allowing the choice of ‘other’ in a majority of the questions with an encouragement for respondents to elaborate on ‘other’ answers. The intention was to use this information to collect data that could be analyzed qualitatively. It was felt that because of the recency of the topic, many of the respondents would need time to consider their answers if these proved to be different than the answer options provided. For this reason, interviews which are more synonymous with qualitative studies were not used. However, in most cases it was found that, respondents only chose to answer with the provided options and hardly made use of the ‘comment’ option. The reason for this can be attributed to the fact that respondents did not yet have enough knowledge about the topic. Additionally, the survey results revealed that the adoption of BYOD is high throughout most of the institutions that took part, despite many of the respondents acknowledging that the practice introduced additional data loss risks. Despite this, most of the institutions had not implemented common technical and administrative controls to minimize these risks. A similar study that involved more qualitative methods such as interviews could expand on the reasons for these lack of controls. With the topic now being less contemporary, interviews, in respect of this type of research, would produce interesting results.

In Chapter 3 the issue of mobile malware was extensively deliberated on. It was discovered that this growing issue was caused by a lack of standardization across the various mobile platforms with a lack of rules for software distribution by developers. In some platforms, there is minimal testing for malicious behaviour in submitted applications and in other platforms, testing techniques are more rigorous but the details thereof are not disclosed. It is believed that if mobile platform vendors were governed by security specific guidelines and thereby certified, users would be able to get the same secure experience from their preferred platform. For this reason, research around the practices for software distribution standards for mobile devices could make for interesting research and improvements for mobile device security.

Finally, it was shown throughout this study that mobile device users increasingly want to use their smartphones or tablet PC's for business purposes. In fact, this need has now transformed into the norm, with employers or more specifically the respective IT Departments no longer being the provider of choice for user technology. With that in mind, some of the studies referenced in this document, have shown that smartphone users are mostly unaware of the security issues pertaining to the devices which they make use of for personal, and more recently business use. Many of the opinions of the technical representatives were that awareness programs are essential to a good security strategy and as such, an interesting research topic would be a comparison of employee awareness to the information security related threats on traditional desktop computing platforms versus their security awareness of similar threats on mobile devices. Such a study would help determine if security awareness on mobile devices needs specific attention. This could lead to the development of mobile device security awareness programs which could be incorporated into both business and educational environments.

8.3. Final Word

The use of personally-owned devices for work related purposes is not an entirely recent observation. This practice has occurred even before the current mobile computing options that are available today. Recent mobile devices such as smartphones and tablet PC’s have however exacerbated the extent of the occurrence BYOD. This has now lead to a realization of the privacy and data loss concerns surrounding this practice.

The development of this project has been a highly educational process for the researcher and it is hoped that this thesis expands this debate. If there is any takeaway from this research, it is that finding a solution to the security concerns that are introduced into organizations that make use of personally-owned mobile devices is not a simple one. Large organizations would need to implement a range of different physical, technical and administrative controls that are developed together as a holistic strategy to effectively minimize the related threats to organizational information assets. For universities, this situation is even harder to maintain given the open information sharing nature of the organizations. South African universities, as evidenced by this research, are as expected, very accepting of mobile device use for work-related purposes, but at the same time have mostly not implemented security controls to minimize these threats. It is hoped that this research elevates the need for effective mobile security strategies within organizations but also for the mobile industry platform vendors and other researchers to come up with solutions to the concerns which were highlighted in this research project.

References

[1] E. B. Koh, J. Oh, and C. Im, “A study on security threats and dynamic access control technology for BYOD, smart-work environment,” in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, 2014, vol. 2.

[2] D. Courbanou, “Dell, Intel: BYOD Is productivity powerhouse | Channelnomics,” 2012. [Online]. Available: http://channelnomics.com/2012/07/26/dell-shows-byod-productivity-powerhouse/. [Accessed: 21-Oct-2012].

[3] M. Zalaznick, “Cyberattacks on the rise in higher education,” *University Business Magazine*, 2013. [Online]. Available: http://www.universitybusiness.com/article/cyberattacks-rise-higher-education. [Accessed: 08-Oct-2014].

[4] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, “Social phishing,” *Commun. ACM*, vol. 50, no. 10, pp. 94–100, 2007.

[5] K. Johnson, “The urgent need for mobile device security policies.,” 2011. [Online]. Available: http://www.infosecisland.com/blogview/18240-The-Urgent-Need-for-Mobile-Device-Security-Policies.html. [Accessed: 21-Oct-2012].

[6] SANReN, “SANReN - About us.” .

[7] TENET, “The Tertiary Education and Research Network of South Africa,” 2013. .

[8] B. Kerievsky, “Security and confidentiality in a university computer network,” *SIGUCCS Newsl.*, vol. 6, no. 3, pp. 9–11, Sep. 1976.

[9] Y. Rezgui and A. Marks, “Information security awareness in higher education: An exploratory study,” *Comput. Secur.*, vol. 27, no. 7–8, pp. 241–253, 2008.

[10] J. R. Vacca, *Computer and Information Security Handbook*. Morgan Kaufmann, 2009.

[11] The University of Maryland, “UMD data breach,” 2014. [Online]. Available: http://www.umd.edu/datasecurity/. [Accessed: 24-Jan-2015].

[12] M. O’Neil, “Data breaches put a dent in colleges’ finances as well as reputations,” *The Chronicle of Higher Education*, 2014. [Online]. Available: http://chronicle.com/article/Data-Breaches-Put-a-Dent-in/145341/. [Accessed: 24-Jan-2015].

[13] J. Roman, “Add butler university to breach list,” *Data Breach Today*, 2014. [Online]. Available: http://www.databreachtoday.com/add-butler-university-to-breach-list-a-7007. [Accessed: 24-Jan-2015].

[14] D. R. Garrison and H. Kanuka, “Blended learning: Uncovering its transformative potential in higher education,” *internet High. Educ.*, vol. 7, no. 2, pp. 95–105, 2004.

[15] W. H. Baker and L. Wallace, “Is information security under control?: Investigating quality in information security management,” *Secur. Privacy, IEEE*, vol. 5, no. 1, pp. 36–44, 2007.

[16] M. Berndtsson, J. Hansson, and B. Olsson, *Planning and implementing your final year project with success: A guide for students in Computer Science and Information Systems*. Springer, 2002.

[17] M. T. Dlamini, J. H. P. Eloff, and M. M. Eloff, “Information security: The moving target,” *Comput. Secur.*, vol. 28, no. 3, pp. 189–198, 2009.

[18] Computer History Museum, “Timesharing Computers,” 2014. [Online]. Available: http://www.computerhistory.org/revolution/networking/19/399. [Accessed: 06-Aug-2014].

[19] M. Campbell-Kelly, “Historical reflections The rise, fall, and resurrection of software as a service,” *Commun. ACM*, vol. 52, no. 5, pp. 28–30, 2009.

[20] F. Avolio, “Firewalls and Internet security, the second hundred (Internet) years,” *Internet Protoc. J.*, vol. 2, no. 2, pp. 24–32, 1999.

[21] D. M. Kienzle and M. C. Elder, “Recent worms: a survey and trends,” in *Proceedings of the 2003 ACM workshop on Rapid malcode*, 2003, pp. 1–10.

[22] M. Gast, *802.11 wireless networks: the definitive guide*. O’Reilly Media, Inc., 2005.

[23] I. Sager, “Before iPhone and Android came Simon, the first smartphone - Businessweek,” *businessweek.com*. [Online]. Available: http://www.businessweek.com/articles/2012-06-29/before-iphone-and-android-came-simon-the-first-smartphone. [Accessed: 10-Sep-2014].

[24] S. N. Foley and R. Dumigan, “Are handheld viruses a significant threat?,” *Commun. ACM*, vol. 44, no. 1, pp. 105–107, Jan. 2001.

[25] W. Lehr and L. W. McKnight, “Wireless internet access: 3G vs. WiFi?,” *Telecomm. Policy*, vol. 27, no. 5, pp. 351–370, 2003.

[26] A. Mylonas, S. Dritsas, B. Tsoumas, and D. Gritzalis, “Smartphone security evaluation - The malware attack case.,” *SECRYPT*, vol. 11, pp. 25–36, 2011.

[27] S. Babin, *Developing software for Symbian OS 2nd Edition: A beginner’s guide to creating Symbian OS v9 smartphone applications in C++*. John Wiley & Sons, 2008.

[28] N. Leavitt, “Mobile phones: the next frontier for hackers?,” *Computer (Long. Beach. Calif).*, vol. 38, no. 4, pp. 20–23, 2005.

[29] Nokia, “Open letter from CEO Stephen Elop, Nokia and CEO Steve Ballmer, Microsoft - conversations,” 2011. [Online]. Available: http://conversations.nokia.com/2011/02/11/open-letter-from-ceo-stephen-elop-nokia-and-ceo-steve-ballmer-microsoft/. [Accessed: 24-Sep-2014].

[30] D. Barrera, P. Van Oorschot, and P. Van Oorschot, “Secure software installation on smartphones,” *IEEE Secur. Priv.*, vol. 9, no. 3, pp. 42–48, 2011.

[31] RIM, “Research In Motion reports fourth quarter and year-end results for fiscal 2009,” 2009.

[32] Statista, “Blackberry smartphone shipments worldwide 2007 to 2013.” [Online]. Available: http://www.statista.com/statistics/263395/rim-smartphones-shipped-worldwide-since-1st-quarter-2007/. [Accessed: 02-Dec-2014].

[33] Apple Inc, “Apple - Press Info - Apple reinvents the phone with iPhone,” 2007. [Online]. Available: https://www.apple.com/pr/library/2007/01/09Apple-Reinvents-the-Phone-with-iPhone.html. [Accessed: 25-Sep-2014].

[34] M. Kenney and B. Pon, “Structuring the smartphone industry: is the mobile internet OS platform the key?,” *J. Ind. Compet. Trade*, vol. 11, no. 3, pp. 239–261, 2011.

[35] Canalys, “64 million smart phones shipped worldwide in 2006 | Canalys,” *Canalys Newsroom*, 2006. [Online]. Available: http://www.canalys.com/newsroom/64-million-smart-phones-shipped-worldwide-2006#. [Accessed: 27-Sep-2014].

[36] Statista Inc, “Smartphones: global shipments 2009-2013,” 2013. [Online]. Available: http://www.statista.com/statistics/271491/worldwide-shipments-of-smartphones-since-2009/. [Accessed: 04-Oct-2014].

[37] Statista Inc, “Smartphone OS: global market share 2009-2013, by quarter | Statista,” 2013. [Online]. Available: http://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/. [Accessed: 28-Sep-2014].

[38] O. H. Alliance, “Alliance Members | Open Handset Alliance.” [Online]. Available: http://www.openhandsetalliance.com/oha_members.html. [Accessed: 30-Sep-2014].

[39] A. Hoog, *Android forensics: investigation, analysis and mobile security for Google Android*. Elsevier, 2011.

[40] R. V. Aroca and L. M. G. Gonçalves, “Towards green data centers: A comparison of x86 and ARM architectures power efficiency,” *J. Parallel Distrib. Comput.*, vol. 72, no. 12, pp. 1770–1780, Dec. 2012.

[41] B. Smith, “ARM and Intel battle over the mobile chip’s future,” *Computer (Long. Beach. Calif).*, vol. 41, no. 5, pp. 15–18, 2008.

[42] Android Central, “Google Play Store now replacing Android Market over-the-air,” 2012. [Online]. Available: http://www.androidcentral.com/google-play-store-now-replacing-android-market-over-air. [Accessed: 01-Oct-2014].

[43] J. Cipriani, “Getting started with ‘User Accounts’ on Android 5.0 Lollipop,” *CNET*, 2014. [Online]. Available: http://www.cnet.com/how-to/getting-started-with-user-accounts-on-android-5-0-lollipop/. [Accessed: 04-Oct-2015].

[44] R. van der Berg, “SA cloud firm takes aim at desktop,” 2014. [Online]. Available: http://www.cloudware.co.za/news/entry/sa-cloud-firm-takes-aim-at-desktop-techcentral#.VH-rz8nPdq4. [Accessed: 04-Dec-2014].

[45] A. K. Talukdar, *Mobile Computing, 2E*. Tata McGraw-Hill Education, 2010.

[46] Microsoft, “Windows Phone SDK 8.0,” *Microsoft Download Center*. [Online]. Available: http://www.microsoft.com/en-za/download/details.aspx?id=35471. [Accessed: 04-Oct-2014].

[47] Gartner Inc., “Gartner 2013 Smartphone sales report,” *Gartner Newsroom,* 2013. [Online]. Available: http://www.gartner.com/newsroom/id/2573415. [Accessed: 30-Sep-2014].

[48] T. Warren, “Google touts one billion active Android users per month,” *The Verge*, 2014. [Online]. Available: http://www.theverge.com/2014/6/25/5841924/google-android-users-1-billion-stats. [Accessed: 05-Dec-2014].

[49] C. Trout, “Apple’s WWDC 2014 in numbers: 800 million iOS devices,” *endgadget.com*, 2014. [Online]. Available: http://www.engadget.com/2014/06/02/apples-wwdc-2014-in-numbers-40-million-on-mavericks-and-more/. [Accessed: 06-Dec-2014].

[50] G. Disterer and C. Kleiner, “BYOD Bring Your Own Device,” *Procedia Technol.*, vol. 9, pp. 43–53, 2013.

[51] D. Maslennikov, “Find and Call: Leak and Spam - Securelist,” 2012. [Online]. Available: http://securelist.com/blog/incidents/33544/find-and-call-leak-and-spam-57/. [Accessed: 28-Sep-2014].

[52] A. Apvrille, “The evolution of mobile malware,” *Comput. Fraud Secur.*, vol. 2014, no. 8, pp. 18–20, Aug. 2014.

[53] B. Lebek, K. Degirmenci, and M. H. Breitner, “Investigating the Influence of Security, Privacy, and Legal Concerns on Employees’ Intention to Use BYOD Mobile Devices,” 2013.

[54] Microsoft, “Satya Nadella email to employees on first day as CEO,” *Microsoft News Center*, 2014. [Online]. Available: http://news.microsoft.com/2014/02/04/satya-nadella-email-to-employees-on-first-day-as-ceo/. [Accessed: 04-Nov-2014].

[55] Goode Intellegence, “Goode Intellegence 2011 Mobile Security Survey Report,” 2011.

[56] T. Claburn, “iPad University: IT Lessons from college pilot - InformationWeek,” 2012. [Online]. Available: http://www.informationweek.com/mobile/mobile-devices/ipad-university-it-lessons-from-college-pilot/d/d-id/1107059? [Accessed: 14-Oct-2014].

[57] R. Langford, “iPhone for monitoring neuromuscular function,” *Anaesthesia*, vol. 67, no. 5, pp. 552–553, 2012.

[58] M. Bell, “Considerations when implementing a BYOD strategy,” *IS Pract. SME Success Ser.*, p. 19.

[59] B. Y. M. Hypponen and M. Hypponen, “Malware goes mobile,” *Sci. Am.*, vol. 295, no. 5, pp. 70–77, 2006.

[60] S. Coursen, “The future of mobile malware,” *Netw. Secur.*, vol. 2007, no. 8, pp. 7–11, 2007.

[61] C. A. Castillo, "Android malware past, present, and future," *White Pap. McAfee Mob. Secur. Work. Gr.*, 2011.

[62] A.-D. Schmidt, H.-G. Schmidt, J. Clausen, K. A. Yuksel, O. Kiraz, A. Camtepe, and S. Albayrak, "Enhancing security of linux-based android devices," in *in Proceedings of 15th International Linux Kongress. Lehmann*, 2008.

[63] J. D'Aguanno, "Blackjacking - 0wning the Enterprise via the BlackBerry," 2006.

[64] P. Estavillo, "ZeuS targets mobile users - Malware Blog, Trend Micro," 2011. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/zeus-targets-mobile-users/. [Accessed: 25-Sep-2014].

[65] A. Mylonas, B. Tsoumas, S. Dritsas, and D. Gritzalis, "A secure smartphone applications roll-out scheme," in *Trust, Privacy and Security in Digital Business*, Springer, 2011, pp. 49–61.

[66] Apple Inc., "Code Signing - Apple Developer Support." [Online]. Available: https://developer.apple.com/support/technical/code-signing/. [Accessed: 21-Dec-2014].

[67] A. Apvrille, "iOS malware does exist," *Fortinet*, 2014. [Online]. Available: https://blog.fortinet.com/post/ios-malware-does-exist. [Accessed: 17-Dec-2014].

[68] C. Xiao and Palo Alto Networks, "WireLurker: A new era in iOS and OS X Malware," 2014. [Online]. Available: https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf. [Accessed: 18-Dec-2014].

[69] M. Egele, C. Kruegel, E. Kirda, and G. Vigna, "PiOS: Detecting privacy leaks in iOS applications.," in *NDSS*, 2011.

[70] Google, "Signing your applications - Android Developer," *Android SDK*. [Online]. Available: http://developer.android.com/tools/publishing/app-signing.html. [Accessed: 30-Sep-2014].

[71] T. Vidas, D. Votipka, and N. Christin, "All your Droid are belong to us: A survey of current Android attacks.," in *WOOT*, 2011, pp. 81–90.

[72] P. McDaniel and W. Enck, "Not so great expectations: Why application markets haven't failed security," *Secur. Privacy, IEEE*, vol. 8, no. 5, pp. 76–78, 2010.

[73] H. Lockheimer and Google Inc, "Android and Security," *Official Google Mobile Blog*, 2012. [Online]. Available: http://googlemobile.blogspot.com/2012/02/android-and-security.html. [Accessed: 18-Dec-2014].

[74] H. Pieterse and M. S. Olivier, "Android botnets on the rise: Trends and characteristics," in *Information Security for South Africa (ISSA), 2012*, 2012, pp. 1–5.

[75] Lookout Inc, "Security Alert: Geinimi, sophisticated new Android trojan found in wild," *Lookout Blog*, 2010. [Online]. Available: https://blog.lookout.com/blog/2010/12/29/geinimi_trojan/. [Accessed: 01-Oct-2014].

[76] Y. Zhou, Z. Wang, W. Zhou, and X. Jiang, “Hey, you, get off of my market: Detecting malicious apps in official and alternative Android markets,” in *Proc. of the 19th Annual Network and Distributed System Security Symposium (NDSS)*, 2012.

[77] X. Jiang, “Security Alert: Stealthy Android spyware - Plankton - found in official Android market,” 2011. [Online]. Available: http://www.csc.ncsu.edu/faculty/jiang/Plankton/. [Accessed: 18-Dec-2014].

[78] D. M. Kurt Baumgartner, Costin Raiu, “Android trojan found in targeted attack - Securelist,” *Securleist*, 2013. [Online]. Available: http://securelist.com/blog/incidents/35552/android-trojan-found-in-targeted-attack-58/. [Accessed: 17-Dec-2014].

[79] M. Stroh, “How Windows Phone guards against malware,” 2013. [Online]. Available: http://blogs.windows.com/bloggingwindows/2013/08/29/how-windows-phone-guards-against-malware/. [Accessed: 18-Dec-2014].

[80] D. Tapellini, “Smartphone thefts rise,” *consumerreports.org*, 2014. [Online]. Available: http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm. [Accessed: 20-Dec-2014].

[81] A. Mylonas, A. Kastania, and D. Gritzalis, “Delegate the smartphone user? Security awareness in smartphone platforms,” *Comput. Secur.*, vol. 34, pp. 47–66, May 2013.

[82] K. Munro, “Android scraping: accessing personal data on mobile devices,” *Netw. Secur.*, vol. 2014, no. 11, pp. 5–9, Nov. 2014.

[83] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, “Smudge attacks on smartphone touch screens.,” *WOOT*, vol. 10, pp. 1–7, 2010.

[84] J. Hong, “The state of Phishing attacks,” *Commun. ACM*, vol. 55, no. 1, pp. 74–81, Jan. 2012.

[85] J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cybersecurity,” *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, Aug. 2014.

[86] H. Xue, T. Wei, and Y. Zhang, “Masque Attack: All your iOS apps belong to us,” 2014. [Online]. Available: https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html. [Accessed: 19-Dec-2014].

[87] Juniper Networks, “2011 Mobile Threats Report - Juniper Networks,” 2011.

[88] G. K. Jayasinghe, J. Shane Culpepper, and P. Bertok, “Efficient and effective realtime prediction of drive-by download attacks,” *J. Netw. Comput. Appl.*, vol. 38, pp. 135–149, Feb. 2014.

[89] R. Naraine, “Mobile Pwn2Own: iPhone 4S hacked by Dutch team,” 2012. [Online]. Available: http://www.zdnet.com/article/mobile-pwn2own-iphone-4s-hacked-by-dutch-team/. [Accessed: 20-Dec-2014].

[90] NIST, “National Vulnerability Database.” [Online]. Available: https://nvd.nist.gov/home.cfm. [Accessed: 20-Dec-2014].

[91] M. Silic and A. Back, “Shadow IT – A view from behind the curtain,” *Comput. Secur.*, vol. 45, pp. 274–283, Sep. 2014.

[92] S. Mansfield-Devine, “Interview: BYOD and the enterprise network,” *Comput. Fraud Secur.*, vol. 2012, no. 4, pp. 14–17, Apr. 2012.

[93] Cisco, “Cisco South African BYOD Research,” *Cisco Newsroom*, 2014. [Online]. Available: http://www.cisco.com/web/ZA/press/2014/082514.html. [Accessed: 05-Oct-2014].

[94] Juniper Networks, “Trusted Mobility Index,” 2012.

[95] Kaspersky, “Global Corporate IT Security Risks : 2013,” 2013.

[96] M. Sunner, “The rise of targeted trojans,” *Netw. Secur.*, vol. 2007, no. 12, pp. 4–7, Dec. 2007.

[97] K. Johnson, “SANS Mobility / BYOD Security Survey,” 2012.

[98] Kevin Johnson and Tony DeLaGrange, “SANS Survey on Mobility/BYOD Security Policies and Practices,” 2012.

[99] N. F. Doherty, L. Anastasakis, and H. Fulford, “Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy,” *Int. J. Inf. Manage.*, vol. 31, no. 3, pp. 201–209, Jun. 2011.

[100] S. Allam, S. V. Flowerday, and E. Flowerday, “Smartphone information security awareness: A victim of operational pressures,” *Comput. Secur.*, vol. 42, pp. 56–65, May 2014.

[101] G. Thomson, “BYOD: enabling the chaos,” *Netw. Secur.*, vol. 2012, no. 2, pp. 5–8, Feb. 2012.

[102] R. A. Stebbins, *Exploratory research in the social sciences*, vol. 48. Sage, 2001.

[103] A. Bhattacherjee, “Social science research: principles, methods, and practices,” 2012.

[104] R. B. Johnson and A. J. Onwuegbuzie, “Mixed methods research: A research paradigm whose time has come,” *Educ. Res.*, vol. 33, no. 7, pp. 14–26, 2004.

[105] L. Cohen, L. Manion, and K. Morrison, *Research Methods in Education*, Sixth Edit. London: Routledge, 2007.

[106] K. B. Wright, “Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services,” *J. Comput. Commun.*, vol. 10, no. 3, p. 0, 2005.

[107] L. Kanuk and C. Berenson, “Mail Surveys and Response Rates: A Literature Review,” *J. Mark. Res.*, vol. 12, no. 4, pp. pp. 440–453, 1975.

[108] P. M. Boynton and T. Greenhalgh, “Selecting, designing, and developing your questionnaire,” *Bmj*, vol. 328, no. 7451, pp. 1312–1315, 2004.

[109] T. W. Miller and P. R. Dickson, “On-line Market Research,” *Int. J. Electron. Commer.*, vol. 5, no. 3, pp. 139–167, Mar. 2001.

[110] D. S. Walonick, “A Selection from Survival Statistics,” *StatPac, Inc*, 2010. [Online]. Available: https://www.statpac.com/surveys/surveys.pdf. [Accessed: 08-Feb-2015].

[111] B. Gillham, *Developing a questionnaire*, Second Edi. A&C Black, 2008.

[112] G. Iarossi, *The power of survey design: A user’s guide for managing surveys, interpreting results, and influencing respondents*. World Bank Publications, 2006.

[113] J. Kirk, “How much should you spend on IT security?,” *InfoWorld*, 2010. [Online]. Available: http://www.infoworld.com/article/2626219/security/how-much-should-you-spend-on-it-security-.html. [Accessed: 24-Feb-2015].

[114] University of Maryland, “Office of Undergraduate Admissions,” 2014. [Online]. Available: http://www.admissions.umd.edu/about/JustTheFacts.php. [Accessed: 25-Feb-2015].

[115] N. Leavitt, “Mobile security: finally a serious problem?,” *Computer (Long. Beach. Calif).*, vol. 44, no. 6, pp. 11–14, 2011.

[116] J. Choobineh, G. Dhillon, M. R. Grimaila, and J. Rees, “Management of information security: Challenges and research directions,” *Commun. Assoc. Inf. Syst.*, vol. 20, no. 1, p. 57, 2007.

[117] S. Young and D. Aitel, *The Hacker’s Handbook: The Strategy behind Breaking into and Defending Networks*. Auerbach Publications, 2004.

[118] F. B. Schneider, “Enforceable security policies,” *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 1, pp. 30–50, 2000.

[119] A. Vance, M. Siponen, and S. Pahnila, “Motivating IS security compliance: Insights from Habit and Protection Motivation Theory,” *Inf. Manag.*, vol. 49, no. 3–4, pp. 190–198, May 2012.

[120] B. Von Solms and R. Von Solms, “The 10 deadly sins of information security management,” *Comput. Secur.*, vol. 23, no. 5, pp. 371–376, 2004.

[121] E. Mills, “In their words: Experts weigh in on Mac vs. PC security,” *CNET*, 2010. [Online]. Available: http://www.cnet.com/news/in-their-words-experts-weigh-in-on-mac-vs-pc-security/.

[122] M. Souppaya and K. Scarfone, “Guidelines for managing the security of mobile devices in the Enterprise,” 2013.

[123] P. Steiner, “Going beyond mobile device management,” *Comput. Fraud Secur.*, vol. 2014, no. 4, pp. 19–20, Apr. 2014.

[124] G. V. Hulme, “Can threat modeling keep security a step ahead of the risks?,” *CSO Online*, 2014. [Online]. Available: http://www.csoonline.com/article/2134353/strategic-planning-erm/can-threat-modeling-keep-security-a-step-ahead-of-the-risks-.html. [Accessed: 28-Feb-2015].

[125] A. Locsin, “Is air travel safer than car travel?,” *USA Today*. [Online]. Available: http://traveltips.usatoday.com/air-travel-safer-car-travel-1581.html. [Accessed: 28-Feb-2015].

[126] Apple Inc., “About Profile Manager.” [Online]. Available: https://help.apple.com/serverapp/mac/4.0/#/apd0E2214C6-50F0-48C9-A482-74CEA1D77A9F. [Accessed: 01-Mar-2015].

[127] K. Hess, “Mobile Management Solutions: MDM vs. MAM vs. MCM,” *tom’s IT Pro*, 2014. [Online]. Available: http://www.tomsitpro.com/articles/evaluating-mobile-management-solutions,2-708-2.html. [Accessed: 01-Mar-2015].

[128] S. Suzuki, Y. Shinjo, T. Hirotsu, K. Itano, and K. Kato, “Capability-based egress network access control by using DNS server,” *J. Netw. Comput. Appl.*, vol. 30, no. 4, pp. 1275–1282, Nov. 2007.

Appendix A - Research Questions and Questionnaire Objectives

1. **Do universities have sensitive data that is worth protecting? What security risks are universities faced with and do personally-owned mobile devices increase this risk? (Secondary research question)** *Addressed in the literature survey – Chapter 2 (Section 2.1) (Summary Below)*

   Universities accumulate a large amount of both personal and financial data that it is of value if compromised. Examples of these are:

   - Research Information
   - Salary Records
   - Alumni Records
   - Student Academic Records
   - Investigative Records
   - ICT Network infrastructure plans
   - User Authentication Data
   - Staff and Student Personally Identifiable Information
   - Financial Records
   - Health Records
   - Credit Card Information

   These are worth protecting because leakage of this information could be used for various criminal activities such as identity theft, intellectual property theft and financial fraud, thus causing the institutions in reputational damage, financial losses and unnecessary expensive litigation. Data such as Personally Identifiable Information is also protected by government legislation such as the POPI act. All South African institutions are governed by such laws and face fines if data leakage of this private information occurs and the institution has not implemented adequate measures of protection.

Several reports show examples data loss from cyber-attacks and the resulting financial implications and impact this has had on universities in the United States. A particular incident involved the physical theft of desktop computers from the University of San Francisco, which contained medical records and personally identifiable information. As a result, the university involved was forced to conduct investigations and offered the affected individuals costly credit monitoring services to avoid litigation. In a similar manner, if personally-owned mobile devices contained such information and was lost or stolen, this would be considered data leakage and the organization could be held responsible. This likelihood for theft or loss is increased by mobile devices due to their portability and size. Additionally, organizations currently have less control over personally-owned mobile devices because the devices are owned by the user and because the device management options, unlike traditional desktops have not yet matured into robust security focused technologies.

Findings from literature: Universities store sensitive data (e.g. personally identifiable information; research information; financial records, etc.). Leakage of such information has resulted in financial losses and reputational damage for both the organization as well as its staff and students. Mobile devices, if allowed to store such data, increase the likelihood of information security risks and data leakage due to their potential for theft/loss as well as lack of organizational device control.

Limitations of literature: Most reports of data loss are reported by universities in the United States. These Reports were caused mostly by traditional endpoint computing devices and not mobile devices. Such reports from South African universities are largely unavailable.

Questionnaire Objective: Are South African universities addressing the additional risks introduced by personally-owned mobile devices by restricting their access to internal, sensitive and restricted data?

2. **What is BYOD? Define the concept and explore the sudden interest of employee's using personal mobile devices for work related purposes. (Secondary research question)** *Addressed in the literature survey – Chapter 2 (Section 2.2) (Summary Below)*

BYOD describes the practice of employees using personally-owned technology such as smartphones and tablet PC's, for work related purposes. Computing technologies have physically transformed from large computing servers and mainframes, down to much smaller personal computers and even smaller eventually into mobile computing handheld devices such as tablet PC's and smartphones. The shift toward mobile computing has also been assisted by supporting mobile broadband technologies such as Wi-Fi and 3G mobile data networks which broaden the scope even further by allowing access to information from almost any location at any time.

Similarly to the evolution of computer use from mainframes to personal computers due to advancements in technology, both the hardware and software of current smartphones and tablet computers have advanced in recent years to such an extent that they are being used for computing purposes that were originally only possible on traditional personal computers. These technologies were originally consumer targeted products but the benefits of continuous access to information from convenient portable handheld computing devices has translated the device popularity into business use as well.

This usability has led to widespread adoption of personal mobile technologies such as smartphones and tablet PC's. Mobile device hardware vendors generally use the same operating system on both their smartphone and tablet operating systems. The most prevalent of these mobile operating systems in order of global pervasiveness today are:

- Google's Android
- Apple's iOS
- Microsoft's Windows Mobile
- RIM's BlackBerry

Direct benefits such as having continuous access to information via mobile devices increase the likelihood of employees using them to access work-related information. These technology advancements have allowed smartphones and tablets to become handheld computing devices and illustrate that it is worth assessing the risks associated with mobile devices.

Findings from literature: Advancements in Internet wireless connectivity such as WiFi 802.11 and 3G networks and their associated improvements on data transfer speeds allow mobile device users continuous access to information. This combined with hardware and software device advancements have assisted Smartphone and Tablet PC's to become useful portable computing devices. While initially designed as personal consumer devices because of their evolution from feature phones, Smartphone usability as computing devices have been realised by employees who want to make use of this functionality to access work-related information, a concept defined by the acronym BYOD. This mobile computing functionality has led to widespread global proliferation of Smartphone and Tablet PC users and therefore increases the probability of employees using them to access sensitive work-related information.

Limitations of literature: Reports of BYOD pervasiveness throughout all industries is very apparent, however their use within universities for work or academic purposes are not available.

Questionnaire Objective: Are personally-owned smartphones and tablet PC's being used for work related and educational purposes in South African universities? If so, how pervasive is this usage?

3. **What are the current acceptance levels of BYOD within organizations and does this compare to the acceptance levels within South African higher education institutions? (Secondary research question)** *Addressed in the literature survey – Chapter 2 (Section 2.3) (Summary Below)*

Various industry related surveys provide an indication that mobile device adoption is evident in different industries globally. Employees are using their personally-owned mobile devices to access business related information with or without the permission of their employers. Universities are not an exception and both employees and students have found imaginative uses for smartphones and tablet PC's.

Staff make use of mobile devices for general computing purposes such as email retrieval when away from the office and in some cases even use them with specialized proprietary mobile applications that allow processing of data from remote locations. Students have found use cases for mobile devices within research by developing mobile applications which extend their functionality for such use. Some universities have even provided tablet PC's to students, the costs of which are included into student fees with the intention of the devices eventually being a replacement for textbooks.

Findings from literature: Evidence of BYOD adoption within organizations globally are presented. Through evidence in academic literature, reports and other sources, some evidence of this adoption within universities is also apparent providing the institutions with various advantageous mobile computing options.

Limitations of literature: This adoption is however mostly user driven and does not give evidence of acceptance from IT Divisions or Management within organizations, even less so in South African universities who are not likely to not be as eager for organizational use given the associated information security risks that have been previously discussed.

Questionnaire Objective: What are the organizational acceptance levels of BYOD specific to South African universities given the Information Security risks? Are the respective institutional IT Divisions allowing BYOD use?

4. **What security threats to organizational data are introduced by these personally-owned mobile devices? (Secondary research question)** *Addressed in the literature survey – Chapter 3 (Section 3.1 and 3.2) (Summary Below)*

Chapter 5 discussed mobile malware in depth and revealed that the numbers of mobile malware variants in the form of trojans are increasing in parallel with the widespread increase in smartphone users. Evidence of mobile device malware dates as far back as the year 2000. This is concerning because it shows that a market exists for malicious software on smartphone's. Additionally researchers have proven the possibility of remote device control with the ability to disclose information contained on the devices over the wireless networks that the devices are connected to on some of the more popular mobile device platforms.

Chapter 6 discussed the additional device vulnerabilities, exploitation trends and threats to information security specific to mobile devices. Practical examples of some of these were given which included physical threats such as the ease of loss or theft of the devices due to their smaller size, as well as web based threats such as those used by attackers to exploit operating system vulnerabilities to install malicious software on user's personal devices when browsing affected websites. Examples of social engineering in the form of SMS Phishing were also evidenced through the literature showing the evolutionary nature of cyber-crime to mobile phones and thus demonstrating the reality of the threats that may be introduced into organizations by the use of personally-owned mobile devices.

Findings from literature: Mobile malware variants are increasing in numbers in direct correlation with the increase in popularity of respective device platforms.

Current mobile malware variants have a variety of propagation techniques but is spread mostly through unmoderated application repositories.

Literature provides evidence of mobile malware being used to expose sensitive locally stored data from smartphones to remote servers by devices that are controlled over the network.

Other threats such as physical device theft, social engineering as well as browser based vulnerability exploitation have been demonstrated by researchers showing the evolution of cyber-crime methods shifting to mobile devices and in some cases, allowing attackers to gain access to other network attached endpoints.

Limitations of literature: The literature in this case provides us with abundant evidence of the threats that are introduced by the use of personally-owned mobile devices. However, enough examples of organizational data leakage through mobile devices were not evident. It was felt that the reason for this was because of the recency of the BYOD phenomenon and similarly felt that universities would also not have enough knowledge of such incidents at their institutions. It was therefore decided that the survey would not specifically ask these questions.

Questionnaire Objective: This research question will not be addressed in the survey.

5. **What does the related research inform us about organizational mobile device adoption in relation to BYOD and which strategies are organizations using to mitigate any associated threats? (Secondary research question)** *Addressed in the literature survey – Chapter 4 (Summary Below)*

5.1. "Shadow IT", identified by researchers Silic and Back [91] as a practice which occurs in organizations which describe the concept of using personal technology for work related purposes that has not been granted specific approval from organizational central IT Departments. This concept has some overlap with concepts such as the Consumerization of IT which similarly overlap BYOD. The difference being that 'bring-your-own-device' refers specifically to the personal devices being used for business purposes. Shadow IT enables employees to leverage technology that increases their productivity and enhances collaboration, with the disadvantage that IT security risks are considerably increased. An important conclusion was that while restriction was considered a valid countermeasure, caution should be used as Shadow IT could create benefits and opportunities for the organization.

Findings from literature: Similarities to BYOD were identified in a concept known as Shadow IT, where personal technology is used for work related purposes. The same reasons were cited in that it increases productivity while significantly increases Information Security risks. Restricting the practice was seen as a countermeasure

Limitations of literature: While related research points out the opinion of technical representatives within other industries, it does not indicate what the opinions of University technical staff are in relation BYOD and the information security risks.

Questionnaire Objective: What are the opinions of technical representatives at South African universities with regards to the organizational Information Security risks? Are these risks exacerbated by BYOD?

5.2. Network visibility is strongly recommended as a key strategy for managing BYOD. The ability to understand which devices are being used on the organizational network and the reason for their use cases is seen as one of the first steps organizations need to take before developing risk assessments and policies that allow, restrict or manage BYOD use. If organizations understand the reasons for employees wanting to leverage the specific technologies, then these needs can be addressed. Similarly if users are "security aware" and understand the threats and organizational risks such as data leakage introduced by using personal devices for work related purposes, user policy compliance will increase.

Findings from literature: Network visibility is critical to BYOD management. By determining which device types are being used on organizational networks down to OS and application level, organizations can start building policies around their use. However organizations need to first understand mobile usage scenarios. Additionally, user awareness is cited as a key factor of having a successful BYOD strategy.

Limitations of literature: Literature does not provide answers to the different device types that are currently connected to SA University networks.

Questionnaire Objective: Do South African universities know which devices staff, students and research associates are using to access critical digital business resources?

5.3. Industry related studies also reveal that globally and across a diverse set of industries, only a few organizations have implemented policies to manage mobile device use, with some institutions having no intention of implementing such policies at all. Alarmingly, even though so few organizations have mobile device security policies in place, a high percentage of these organizations have recently experienced mobile related security incidents and leaks of corporate data that involved mobile devices. Additionally, many organizational representatives are in agreement that the policies that address BYOD are very important, even though only a small percentage of these organizations have actually implemented them.

Findings from literature: Drawing from many industry related research studies, many organizational representatives are of the opinion that BYOD policies are very important mitigation strategy for security threats. Despite this, very few organizations globally have fully-implemented such policies at their institutions.

A cross-industry South African survey revealed that almost two thirds of employees were allowed to use personal devices on company networks.

However, very few SA organizations have BYOD polices or their employees were unaware of any such strategies.

Limitations of literature: While there are some reports and industry related surveys to report on the lack of BYOD policies, reports specific to higher education institutions were not available in literature.

Questionnaire Objective: Have South African universities implemented Information Security policies related to mobile devices and BYOD? Are these policies being enforced?

Appendix B – Questionnaire

Security concerns for BYOD in South African Higher Education Institutions

Introduction

This research is undertaken on behalf of Rhodes University for scholarly purposes.

Purpose of Questionnaire:

The primary objective of this questionnaire is to examine the Information Security maturity levels of ICT Departments within South African Higher Education institutions related to the concept of Bring Your Own Device (BYOD) and mobile computing technologies.

Reasons for Research

As mobile computing technology matures, end users are increasingly requesting access to institutional enterprise network data, services and resources from these devices whether issued by the organization or personally-owned. These institutions are under pressure to accept the associated security risks inherent in current mobile devices due to, amongst other factors, perceived costs savings, user desire for convenience and mobility [1]. Although institutional ICT Departments are now becoming more accepting to the concept of BYOD, the controls and policies to ensure integrity, confidentiality and availability of related services are not well defined.

University networking infrastructures have been designed to accommodate staff, students, visitors and researchers with the capability to share large amounts of data between them. As a result, previous studies have shown that University networks have been targeted for two key reasons: firstly because the huge amounts of computing power they hold; and secondly because of their open, often exposed access they provide to their users and in some cases even the public.

This questionnaire has therefore been designed with the intention of gaining insight into what policies and controls are deemed important by evaluating the current Information Security maturity levels within South African HE Institutions relative to the growing mobile device trend.

[1] L. Chen, J. Franklin, A. Regenscheid, and NIST, "Guidelines on Hardware - Rooted Security in Mobile Devices (Draft) Recommendations of the National Institute of Standards and Technology. Special Publication 800-164," vol. 164. p. 33, 2012.

"http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf"

Instructions and Participation Benefits

Please answer all the questions truthfully and to the best of your knowledge and follow the instructions specific to each.

Please direct any queries with regard to this questionnaire or about the research to: email addresses: g.sauls@ru.ac.za (Researcher) or j.connan@ru.ac.za (Supervisor)

Survey results will be announced to all participants and shared amongst the various institutions that have taken part by approximately June 2013. The results may provide insight and assistance when making decisions regarding the policies, controls and Information Security practices related to managing mobile devices within Higher Education institutions.

Confidentiality and Ethics

To help protect your confidentiality, your responses will be confidential and the analyzed data collected will not be linked with any identifying information such as your name, email address or your respective organization/institution within any resulting published report.
The utmost effort is be made to ensure anonymity of your respective Institution.
All data is stored in a password protected electronic database. The results of this study will be used for scholarly purposes only and may be shared with Rhodes University representatives as well as your institution if you have chosen to respond, although no identifying information will be revealed.

All participants are free to withdraw from the project at any time, even after the project commences.
This research has been reviewed according to Rhodes University Ethics procedures for research involving human subjects.

By clicking "*next*" you are indicating that:

- **You have read and understood the above information.**
- **You voluntarily agree to participate.**

There are 40 questions in this survey

Respondent Profiling

This survey has been aimed at respondents employed within South African Higher Education Institutions, on a national scale, holding senior technical positions within their respective ICT Departments.

1 [Q1_HEConfirm] Please confirm that you are employed at a *South African Higher Education* Institution. *

Please choose **only one** of the following:

- ○Yes
- ○No

2 [Q2_OrgRole] What is your organizational role in your institution? *

Please choose **only one** of the following:

- ○ICT Director
- ○ICT Systems Manager
- ○Chief Information Security Officer
- ○ICT Network/System Administrator
- ○ICT Security Services Manager
- ○ICT Security Administrator
- ○Security Analyst
- ○Other

3 [Q3_RespondentExp] How many years of experience do you have in the ICT Field?

Please choose **only one** of the following:

- ○0 – 5
- ○5 – 10
- ○10 – 30
- ○30+

Institutional Profiling

This section assesses the institutions reliance on ICT Services.

4 [Q4_Budget] What is your annual Institutional ICT Budget? ***(in Rands)***
(Estimation is acceptable if exact figures aren't obtainable)

Please write your answer here:

- R …………………..

5 [Q5_SecurityBudget] What is your Institutional annual average spend on ICT Security related services and products e.g AntiVirus, Firewalls etc.? ***(in Rands)***
(Estimation is acceptable if exact figures aren't obtainable)

Please write your answer here:

- R …………………………

6 [Q6_InfoSecOffice] Does your institution have a distinctive section or post for Information Security within the ICT Division? *

Please choose **only one** of the following:

- ○Yes, we have a separate Information Security department that has more than one staff member within our ICT Division.
- ○Yes, we have a specific role for an Information Security Officer within our ICT Division.
- ○No, we do not have a specific section or Information Security Officer role within our ICT Division.
- ○Don't Know.
- ○Other

7 [Q7_StaffCount] What is the staff count of your support and academic staff in your entire organization? (an estimation is acceptable if you are unsure) *

Please choose **only one** of the following:

- ○1 – 500
- ○501 – 1,000
- ○1,001 – 2,500
- ○2,001 – 5,000
- ○5,000 - 10,000
- ○More than 10,000
- ○Don't Know

8 [Q8_StudentCount] What is the student count in your entire organization? (an estimation is acceptable if you are unsure) *

Please choose **only one** of the following:

- ○5,000 - 15,000
- ○15,000 - 25,000

- ○25,000 - 45,000
- ○More than 45,000
- ○Don't Know

9 [Q9_MobileStrategy] Has your institution implemented *any* mobile device strategy regardless of device ownership?
(Please feel free to comment in the box provided if necessary) *

Please choose **only one** of the following:

- ○Yes, fully implemented
- ○Yes, partially implemented
- ○No, not yet implemented
- ○No, no intention
- ○Don't Know

Make a comment on your choice here:

> ***Fully implemented*** means a mobile device strategy has been fully implemented and published throughout the Institution. Only minor additions are to be made if changes are necessary as the institution learns about these.
>
> ***Partially implemented*** refers to a mobile device strategy that is still in its infancy, more guidelines are still to be added as the institution learns about them, although the strategy has been informally published.
>
> ***Not yet implemented*** means that the Institution has not yet implemented a strategy around mobile devices.
>
> ***No intention*** indicates that the institution does not intend to develop a mobile device strategy of any kind.

10 [Q10_BYODstrategy] Has your institution implemented *any* mobile device strategy specific to *user-provisioned* devices?
(Please feel free to comment in the box provided if necessary) *

Please choose **only one** of the following:

- ○Yes, fully implemented
- ○Yes, partially implemented
- ○No, not yet implemented
- ○No, no intention
- ○Don't Know

Make a comment on your choice here:

> ***Fully implemented*** means a mobile device strategy has been fully implemented and published throughout the Institution. Only minor additions are to be made if changes are necessary as the institution learns about these.
>
> ***Partially implemented*** refers to a mobile device strategy that is still in its infancy, more guidelines are still to be added as the institution learns about them, although the strategy has been informally published.
>
> ***Not yet implemented*** means that the Institution has not yet implemented a strategy around mobile devices.
>
> ***No intention*** indicates that the institution does not intend to develop a mobile device strategy of any kind.

Institutional Policies

This section assesses the institutions' policies on usage of ICT services and attempts to compare these with policies and usage specific to BYOD.

11 [Q11_BYODSupport] Do you support *personally-owned,* Internet-capable mobile devices such as smartphones and tablet PC's on your network? *

Please choose **only one** of the following:

- ○Yes, we are changing our network services and content to actively support these devices.
- ○Yes, although limited as we currently offer network access only.
- ○Yes, although limited as we offer network access to limited areas of the institutional network only. (e.g. Internet only)
- ○Somewhat, we only allow specific types of devices on our institutional network.
- ○No, we currently do not allow these devices to connect to our institutional network.
- ○Other

12 [Q12_BYODCount] How many *personally-owned,* Internet-capable *mobile devices* are registered on the institutional network currently?
***(If unsure, an estimation is acceptable)* ***

Please choose **only one** of the following:

- ○None
- ○Less than 10
- ○11 – 100

- ○100 – 250
- ○250 – 1,000
- ○1,000 – 5,000
- ○5,000 - 10,000
- ○more than 10,000
- ○Don't know, currently we have no reliable way to calculate this data

13 [Q13_DevCountIncrease] Would you say that within the last two years, the *number* of personally-owned smartphone and tablet devices connecting to the institutional network has... *

Please choose **only one** of the following:

- ○Decreased slightly
- ○Remained relatively unchanged
- ○Increased slightly
- ○Increased significantly (doubled)
- ○Increased significantly (tripled)
- ○Increased immensely (more than tripled)
- ○Don’t know, currently no way to accurately calculate this data.
- ○Other

14 [Q14_DeviceType] Which *mobile software platforms* are currently being supported/allowed on the institutional network? *

Please choose **all** that apply:

- □RIM Blackberry.
- □Apple iPhone/iPad.
- □Google Android.

- □Windows Mobile.
- □Symbian OS.
- □We do not plan on restricting certain device types.
- □None
- □Other:

15 [Q15_DeviceAccess] What would you describe the level of confidence is, in knowing what types of devices are accessing *business* resources? *

Please choose **only one** of the following:

- ○Not Confident (0%)
- ○Vaguely (0% - 40%)

- ○Fairly (40% - 75%)
- ○Extremely (75 – 99%)
- ○Completely (100%)

16 [Q16_AUP] Does your institution have a *published* Acceptable Use Policy? *

Please choose **only one** of the following:

- ○Yes, Fully Implemented
- ○Yes, Partially Implemented
- ○No, Not Implemented
- ○Don't Know

Fully implemented means the policy has been fully implemented and published throughout the institution. Only minor additions are to be made if changes are necessary as the policy is in full effect.

Partially implemented refers to a policy that is still in its infancy, more rules are still to be added as the institution learns about them, although the policy has been published.

Not implemented means that the organization has not yet, or does not intend to publish this kind of policy.

17 [Q17_SecPol] Does your institution have a *published* Information Security Policy? *

Please choose **only one** of the following:

- ○Yes, Fully Implemented
- ○Yes, Partially Implemented
- ○No, Not Implemented
- ○Don't Know

Fully implemented means the policy has been fully implemented and published throughout the institution. Only minor additions are to be made if changes are necessary as the policy is in full effect.

Partially implemented refers to a policy that is still in its infancy, more rules are still to be added as the institution learns about them, although the policy has been published.

Not implemented means that the organization has not yet, or does not intend to publish this kind of policy.

18 [Q18_BYODPol] Does your institution have a *published* policy for personally-owned Mobile devices? (Personally-owned refers to devices that have been provisioned by the user's themselves and are therefore not owned by your institution) *

Please choose **only one** of the following:

- ○Yes, Fully Implemented
- ○Yes, Partially Implemented
- ○No, Not Implemented
- ○Don't Know
- ○Other

> ***Fully implemented*** means the policy has been fully implemented and published throughout the institution. Only minor additions are to be made if changes are necessary as the policy is in full effect.
>
> ***Partially implemented*** refers to a policy that is still in its infancy, more rules are still to be added as the institution learns about them, although the policy has been published.
>
> ***Not implemented*** means that the organization has not yet, or does not intend to publish this kind of policy.

19 [Q19_Rating4Controls] Consider the main drivers for implementing policies for personally-owned mobile devices? Please rate the significance for your institution, of each of the following with the scale provided. (This question seeks to answer why creating policies for user provisioned mobile devices were/are necessary). *

Only answer this question if the following conditions are met:
Answer was 'Yes, Fully Implemented' *or* 'Yes, Partially Implemented' *or* 'Other' at question '18 [Q18_BYODPol]' (Does your institution have a published policy for personally-owned Mobile devices? (Personally-owned refers to devices that have been provisioned by the user's themselves and are therefore not owned by your institution)) *and* Answer was 'Yes, Fully Implemented' *or* 'Yes, Partially Implemented' *or* 'Other' at question '18 [Q18_BYODPol]' (Does your institution have a published policy for personally-owned Mobile devices? (Personally-owned refers to devices that have been provisioned by the user's themselves and are therefore not owned by your institution)) *and* Answer was 'Yes, Fully Implemented' *or* 'Yes, Partially Implemented' *or* 'Other' at question '18 [Q18_BYODPol]' (Does your institution have a published policy for personally-owned Mobile devices? (Personally-owned refers to devices that have been provisioned by the user's themselves and are therefore not owned by your institution))

Please choose the appropriate response for each item:

	Irrelevant	Slightly Significant	Significant	Highly Significant
Protecting sensitive information	○	○	○	○
Compliance with Standards	○	○	○	○
Legal compliance (e.g. POPI bill)	○	○	○	○
Enabling Mobile Workers	○	○	○	○
Supporting ICT innovations	○	○	○	○
Defining data ownership	○	○	○	○
Defining level of support	○	○	○	○

Irrelevant, is the lowest rating on the scale, meaning that this was not at all a driving factor for implementing device policies for personally-owned mobile devices.
Slightly significant, is next up from 'Irrelevant', meaning this this was only somewhat a driving factor for implementing device policies for personally-owned mobile devices.
Significant, is next up from 'Slightly significant', meaning this this was a significant driving factor for implementing device policies for personally-owned mobile devices.
Highly Significant, is the highest rating on the scale, meaning that this was a major driving force for implementing device policies for personally-owned mobile devices.

20 [Q20_BYODPolTopics]

The following is a list of some of the topics covered in typical BYOD/Mobile Device policy. Please rate the importance of each of the following from (1 - 5) with 1 being least important and 5 being most important.*

Only answer this question if the following conditions are met:
Answer was 'Yes, Partially Implemented' *or* 'Yes, Fully Implemented' *or* 'Other' at question '18 [Q18_BYODPol]' (Does your institution have a published policy for personally-owned Mobile devices? (Personally-owned refers to devices that have been provisioned by the user's themselves and are therefore not owned by your institution)) *and* Answer was 'Yes, Partially Implemented' *or* 'Yes, Fully Implemented' *or* 'Other' at question '18 [Q18_BYODPol]' (Does your institution have a published policy for personally-owned Mobile devices? (Personally-owned refers to devices that have been provisioned by the user's themselves and are therefore not owned by your institution)) *and* Answer was 'Yes, Partially Implemented' *or* 'Yes, Fully Implemented' *or* 'Other' at question '18 [Q18_BYODPol]' (Does your institution have a published policy for personally-

owned Mobile devices? (Personally-owned refers to devices that have been provisioned by the user's themselves and are therefore not owned by your institution))

Please choose the appropriate response for each item:

	1	2	3	4	5
Access and Authentication	○	○	○	○	○
Acceptable usage/Employee Education	○	○	○	○	○
Configuration (data wipe, passcodes etc.)	○	○	○	○	○
On device stored data	○	○	○	○	○
Data Ownership	○	○	○	○	○
Malware Protection	○	○	○	○	○
Application Use	○	○	○	○	○

21 [Q21_BYODPolControls] Please select the relevant controls introduced in the BYOD/Mobile Device policy.
(If your organization does not yet have an official policy, please select the controls you feel are most important) *

Only answer this question if the following conditions are met:
Answer was 'Yes, Fully Implemented' *or* 'Yes, Partially Implemented' *or* 'Other' at question '18 [Q18_BYODPol]' (Does your institution have a published policy for personally-owned Mobile devices? (Personally-owned refers to devices that have been provisioned by the user's themselves and are therefore not owned by your institution)) *and* Answer was 'Yes, Fully Implemented' *or* 'Yes, Partially Implemented' *or* 'Other' at question '18 [Q18_BYODPol]' (Does your institution have a published policy for personally-owned Mobile devices? (Personally-owned refers to devices that have been provisioned by the user's themselves and are therefore not owned by your institution)) *and* Answer was 'Yes, Fully Implemented' *or* 'Yes, Partially Implemented' *or* 'Other' at question '18 [Q18_BYODPol]' (Does your institution have a published policy for personally-owned Mobile devices? (Personally-owned refers to devices that have been provisioned by the user's themselves and are therefore not owned by your institution))

Please choose **all** that apply:

- □Devices access control for access to Institutional resources.
- □Staff/Students are required to accept usage agreement.
- □Minimal agent-less device management via mobile device sync.
- □Institution ensures security through Mobile Device management Agent.
- □Staff/Students are to secure and monitor their own devices.
- □Application or Institutional Data Sandboxing.
- □Remote Data Wipe capability.
- □Don't know.

- □Other:

22 [Q22_BYODPolValue] How important is incorporating personally-owned mobile device policies into the overall Institutional Security and Compliance framework? *

Please choose **only one** of the following:

- ○Unimportant
- ○Important
- ○Critical
- ○Don’t Know

23 [Q23_PolNonComply] Would you say the consequences of non-compliance of Institutional ICT policies are clearly communicated and enforced? *

Please choose **only one** of the following:

- ○Not Strongly Enforced
- ○Partially Enforced
- ○Strictly Enforced
- ○Don't Know

Management, Controls and Opinion

This section assesses the technical controls currently deployed by the institution to enforce policies related to personally-owned mobile devices.

24 [Q24_BYODStakeholders] ***In your opinion, who do you see as the key stakeholders that should be interested in implementing a BYOD program at your Institution? ****

Please choose **all** that apply:

- □Legal
- □Human Resources
- □Finance
- □Information Technology
- □Don't know
- □Other:

25 [Q25_MitigateStrategy] In your opinion, please rate the importance of each of the current security mitigation tools and strategies that are being used to manage risks associated with mobile endpoints. With 1 being irrelevant and 5 being essential.

Please choose the appropriate response for each item:

	1	2	3	4	5
Employee Education/Awareness	○	○	○	○	○
Log Monitoring	○	○	○	○	○
Mobile Device (Centralized) Management	○	○	○	○	○
Network Access Control (NAC/NAP)	○	○	○	○	○
Virtual Desktop Interface (VDI)	○	○	○	○	○
Endpoint Anti-Malware Protection	○	○	○	○	○
Enforced Application Controls(Whitelisting/Private App Store)	○	○	○	○	○
Intrusion Prevention System (IPS)	○	○	○	○	○
Device Level (local) Encryption	○	○	○	○	○

26 [Q26_LaptopEncryption] Currently in your institution, would you say for laptop computers local disk storage encryption technologies are... *

Please choose **only one** of the following:

- ○Enforced.
- ○Advised or Recommended to users.
- ○Neither enforced nor advised.
- ○Don't know
- ○Other

Examples of encryption technologies includes Microsoft Bitlocker or TrueCrypt (http://www.truecrypt.org/)

27 [Q27_USBEncryption] Currently in your institution, would you say for USB flash drives, local disk storage encryption technologies are... *

Please choose **only one** of the following:

- ○Enforced.
- ○Advised or Recommended to users.
- ○Neither enforced nor advised.
- ○Don't know
- ○Other

Examples of encryption technologies includes Microsoft Bitlocker or TrueCrypt (http://www.truecrypt.org/)

28 [Q28_MobileEncryption] Currently in your institution, would you say for mobile devices, local disk storage encryption technologies are... *

Please choose **only one** of the following:

- ○Enforced.
- ○Advised or Recommended to users.
- ○Neither enforced nor advised.
- ○Don't know
- ○Other

Examples of encryption technologies includes Microsoft Bitlocker or TrueCrypt (http://www.truecrypt.org/)

29 [Q29_OpinionOfTools] What would you describe your current level of satisfaction is with current *Mobile Device Management* solutions, if any?
***(please feel free to leave comments in the box provided if necessary)* ***

Please choose **only one** of the following:

- ○Dissatisfied
- ○Somewhat Satisfied
- ○Satisfied
- ○Very Satisfied
- ○Don't Know

Make a comment on your choice here:

30 [Q30_NegativePositive] In your opinion, the Bring Your Own Device trend introduces... *

Please choose **only one** of the following:

- ○More negative risks than positives and advantages to institutional ICT networks.
- ○More positives and advantages than negative risks to institutional ICT networks.
- ○A similar balance of both risks as well as advantages.
- ○Don't Know
- ○Other

Examples of negatives include security risks such as loss of institutional data, unauthorized access to data, increased attack avenues for malware and malicious groups such as hackers, as well as increased Management and Security spending related costs.

Examples of positives include financial benefits such as increased productivity and reduced spending on computing devices, as well as operational benefits such as mobility of employees, workplace flexibility and increased data sharing.

31 [Q31_SecurityOpinion] When comparing security features of current Smartphone and Tablet PC Operating Systems with traditional Desktop and Laptop Operating Systems *would you say…*
(Please feel free to leave a comment in the box provided if necessary) *

Please choose **only one** of the following:

- ○Traditional Desktop Operating Systems offer better security features than Mobile Operating Systems.
- ○Mobile Operating Systems offer better security features than Desktop and Laptop Operating Systems.
- ○There aren't any remarkable differences in terms of Security, they're equally secure.
- ○Don't know.

Make a comment on your choice here:

32 [Q32_BYODRisk] In your opinion, when we allow Smartphones and Tablet PC's onto institutional networks with access to business resources... *

Please choose **only one** of the following:

- ○The risk of data loss and security breaches is significantly increased over and above traditional risks.
- ○The risk of data loss and security breaches is only slightly increased over and above traditional risks.
- ○The risk of data loss and security breaches over and above traditional risks remains the same and is not at all increased.
- ○Don't know
- ○Other

Laptops and USB Drives as an example, due to their portable nature have long been considered as a risk for potential business data loss; this characteristic is common to Smartphone and Tablet PC's as well, although this does not necessarily indicate it is the only security related concern.

33 [Q33_DataOwnership] Considering that with BYOD, the device itself belongs to the user. With regards to the data however, some of the data which resides on the device may belong to the *user* and some of the data may belong to the *institution*. Keeping this in mind, would you say... *

Please choose **only one** of the following:

- ○The organization is responsible for data security on the device.
- ○The user is responsible for data security on the device.
- ○Both the organization as well as the user share the responsibility for data security on the device.
- ○Don't know
- ○Other

34 [Q34_AntiMalware]Considering the current state of mobile devices and their operating systems, do you feel that anti-malware (e.g. anti-virus software) is necessary on mobile devices before being allowed to access business resources? *

Please choose **only one** of the following:

- ○Yes, anti-virus on mobile devices is just as important as it is on desktop computers.
- ○No, anti-virus is not necessary because mobile devices aren't susceptible to malware as compared to desktop computers.
- ○Don't know
- ○Other

35 [Q35_OSThreatCompare]Would you say that, of the current mobile platform Operating Systems, certain platforms in their normal device state introduce a significantly greater amount of security threats when compared with others? *

Please choose **only one** of the following:

- ○Yes
- ○No
- ○Don't know
- ○Other

Normal device state refers to devices that have not been rooted (Android) or Jailbroken (iOS).

36 [Q36_OSRiskLikelyhood] Please choose from the following mobile platforms, the types of device Operating Systems that are likely to introduce the highest percentage of security threats into the Institutional network. *

Only answer this question if the following conditions are met:
Answer was 'Yes' at question '35 [Q35_OSThreatCompare]' (Would you say that, of the current mobile platform Operating Systems, certain platforms in their normal device state introduce a significantly greater amount of security threats when compared with others?)

Please choose **all** that apply:

- □Apple iOS
- □Microsoft Windows Phone / Tablet
- □RIM Blackberry OS
- □Google Android
- □Symbian
- □Other:

37 [Q37_RatingRestrict] Would the device "high security threat ranking" above in any way influence which types of mobile device platforms would be allowed to access critical business resources? *

Only answer this question if the following conditions are met:
Answer was 'Yes' at question '35 [Q35_OSThreatCompare]' (Would you say that, of the current mobile platform Operating Systems, certain platforms in their normal device state introduce a significantly greater amount of security threats when compared with others?)

Please choose **only one** of the following:

- ○Yes, these device types will not be allowed to access business resources
- ○No, as this would oppose a true BYOD strategy
- ○Don't know
- ○Other

Suggestions

Questions and Suggestions?

38 [Q38_Suggestions] If you have any suggestions you would like to share that have not been represented by the questions please feel free to do so here.

Please write your answer here:

…………………………………………………………………………………………….

> If you're institution has already begun with Implementation of BYOD strategies, please share your experiences here.
> As an example, you may want to express what the most challenging aspects are.
> E.g. Data ownership issues, Device Support issues, Mobile Application Management issues are all relevant concerns. Which of these has been considerably more difficult than others for your institution.

39 [Q39_Clarification] Are you available to contact for further insight or clarification on some of your responses? *

Please choose **only one** of the following:

- ○Yes
- ○No

40 [Q40_Results] Would you like to receive a summary of the results? *

Please choose **only one** of the following:

- ○Yes
- ○No

Thank you for participating