MASTER'S THESIS

Smartphone Information Security Risks

Portable Devices and Workforce Mobility

Esi Maan Nunoo
2013

Master (120 credits)
Master of Science in Information Security

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

LULEÅ UNIVERSITY OF TECHNOLOGY

ACKNOWLEDGEMENT

I thank the Almighty God for giving me the strength, courage, knowledge, wisdom and guidance without which this goal could not have been achieved.

I am indebted to Professor Helena Karasti, for being an inspiring supervisor and a great mentor. I wish to express my sincere gratitude to her for her guidance, criticisms, suggestions and the time she invested in working with me. I have learnt a lot from her.

I am grateful to all the lecturers in my department who in one way or the other offered some form of assistance to me.

I would like to thank the Swedish Armed Forces (SwAF) for giving me the opportunity to work on this study for them. To my external supervisor, Mr. Ross W Tsagalidis thank you for your guidance, criticisms, suggestions and the time you invested in working with me.

Stephen Famurewa, Seth Akonor Adjei and Samuel Ayowole Awe thank you for your immense help. Your discussions and suggestions helped to complete this report.

I would also like to thank my fellow colleagues who helped in criticizing this work. Your constructive criticisms helped refine this piece of work. Thank you.

Finally, I would like to express my gratitude to my family and my friends for their love, understanding, patience and support, all of which made it possible for me to bring this research work to an end.

ABSTRACT

Today's world is characterised by a heavy dependence on information technology and technological devices to perform even the simplest of tasks. While this in itself is not a bad thing, our over dependence and neglect has put us in a situation where the confidentiality, integrity and availability of our information resources are continuously being questioned.

ENISA (2010) report that in the third quarter of 2010 eighty million Smartphones were sold worldwide, with the UK, Germany, France, Spain, and Italy reporting a sixty million increment in the number of smartphone users. Reardon (2007) additionally predicted that between 2007 and 2012 there was going to be a 30% year-on-year growth in the sale of smartphones. The improvement of smartphones together with its rapidly decreasing unit price has placed smartphones within the reach of all employees. Due to the mobile nature of the device, it has brought challenges to the information security needs of organizations. As the sale of smartphone continue to increase so does the number of vulnerabilities on mobile operating systems. Knowing where to place the smartphone is of prime importance in this study. Is it just a socio-technical tool for private use or it must be extended to be used as a working tool? If so, how should it be used to limit the exposure of organizational information?

The study makes use of interviews in finding out what users of the device think about the device and how secure they think their device is. The interviews also tries to find out how securely the users have configured their devices, their mobility rate and what policies have been put in place to help guide users of the device while using the device.

Findings from this study indicate that smartphone threats are diverse, complicated and smart. As the price of the smartphone reduces and their functionality improves, the number of its users increases. This makes it a target for hackers and malware as they can exploit the device to gain personal and organizational data. In spite of this, the perception of users on the risks of using a smartphone for work is not as high as can be. Users still think that if only the phone is used for making and receiving calls, reading and replying to emails and checking calendar schedules, then there is nothing much to protect. In reality this is not the case. Smartphones have a lot more going on them than just the aforementioned. Users must be educated on the reality of the matter and be made aware of the current risks there are so as to increase their consciousness on this matter. Finally, the discussion in this study sheds some light on the challenges that mobility and smartphone usage for work pose to organizational information security.

The choice of a counter measure depends on factors such as what kind of data the organization produces as well as what kind of usage patterns employees have. There is no one size fit all counter measure that can be implemented. Organizations must realize this and embark on the best solutions that are suitable for their organization. To get the best counter measures in place, organizations are advised to make their own risk assessments and weigh the risks against the potential benefits in their own specific cases.

TABLE OF CONTENT

TABLE OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ABBREVIATION	DESCRIPTION
APP	Software application for smartphone or application
App Store	Software distribution channel or market for third-party software
AT&T	American Telephone and Telegraph
BYOD	Bring Your Own Device
ENISA	European Network and Information Security Agency
GPS	Global Positioning System
GSM	Global System for Mobile Communication
IBM	International Business Machines
ICT	Information and Communication Technology
IE	Internet Explorer
IOS	Apple's Mobile Operating System
IT	Information Technology
MMS	Multimedia Messaging Service
PDA	Personal Digital Assistant
PIN	Personal Identification Number
SLR	systematic literature review
SMS	Short Messaging Service
TAM	Technology Acceptance Model
VPN	Virtual Private Network
Wi-Fi	Wireless Local Area Network

CHAPTER ONE

INTRODUCTION

1.1 Background

Today's world is characterised by a heavy dependence on information technology to perform even the simplest of tasks. From household to industry there is an information technology solution for everyone and everything. Today, money transfer can be done on a personal device like the smartphone. We do not have to go far to check our flight details or to read our emails. Cyber Future's market survey by USA Today Magazine (2006) indicates 92 ways in which information technology will change our lives by 2025. Technology will continue to interfere and change human life dramatically but not always for the better. As information technology increases work efficiency and effectiveness (Walton, 1985; Manz & Stewart, 1997; Eason, 2001; Chen & Nath, 2011), we are at the risk of exposing sensitive data to unauthorized persons, as we allow our information and data to travel across various networks using all manner of devices with ubiquitous internet access. This problem becomes even more challenging when employees move from one place to another and work irrespective of where they are through their portable devices. The increasing mobility of workers and the growth of smartphone usage for work due to the device's corresponding growth in application and storage of sensitive data mean a possible breach in perimeter security (Fitzgerald, 2009).

The academic edition of Britannica defines the word "portable" as the ability or capability of being moved especially with ease. From this definition I define a portable device as a device that is small enough to be hand-held and lightweight to be carried around without the stress of feeling that one is carrying an additional load. Laptop computers, PDA's, mobile phones, hand-held computers and Tablet PC's are common examples of portable devices. The word portable could also be referred to as mobile as the two mean the same and can be used interchangeably.

Ernst & Young (2011) state that the advancement of mobile devices has seen a shift of PDA's between 1990 and 2000 to a tremendous increase in smartphone and tablet usage because of its ubiquitous and multi-functional abilities. Portable or mobile devices such as flash drives, personal audio players, smartphones, personal digital assistants and tablets provide a convenient way of accessing business and personal data ubiquitously. This has resulted in increased information leakage. The features of portable devices that make them handy,

convenient and enable them to have a real time connection to various networks and hosts also make them vulnerable to losses of physical control and network security breaches (Ernst & Young, 2011; Walters, 2012).

Takesue (2007) suggests that this is mainly because these devices are used by employees without realizing the dangers they may present when used to carry organizational digital assets both inside and outside the organization. This ignorance could result in the loss of large amounts of an organization's sensitive data when the device is lost or stolen, data exposure when sensitive data is exposed to the public or a third party without consent, and increased exposure to network-based attacks to and from any system the device is connected to both directly and via networks over the internet (Heikkila, 2007; Fratto, (2009); Walters, 2012). Ernst & Young (2011) additionally affirm that the constant access to email and corporate applications using portable devices enable mobile business applications that allow access to and storage of sensitive company data as well as private personal data which eventually could lead to numerous security risks as stated above.

Though portable devices provide ubiquitous connectivity and can increase productivity, the risks that they are associated with has raised concerns as to whether they are indeed a necessary tool for work or just a socio-technical tool for personal use. Whereas laptops and personal computers have numerous antivirus programs to choose from, allow software on them to be updated regularly to make them more secured and have additional settings that allows them to be extra hardened and secured, portable devices such as mobile phones, smartphones and PDA's do not have same features. Ruggiero and Foote (2011) suggest that while security on the traditional computer is matured, security on mobile devices such as phones is still in their infancy. On some portable devices updates can only be made when the providers have made them available. This is true for the traditional computers as well but then the frequency with which updates are made to computers cannot be compared to the frequency with which same is done on portable devices. Portable devices in most cases do not have regular and short time span updates.

Botha, Furnell & Clarke (2009) point out that portable device security has become a point of neglect by most organizations. Whereas organizations have system administrators who take care of configuring computers in the organization to meet optimal security requirements, portable devices such as PDA's, mobile phones and smartphones are usually configured by

users to suite their preferences even when organizations purchased them for work. The problem with this approach is that not all users possess the technical knowledge of how to securely configure their portable devices to support the organizations information security needs. This makes the organization have a weak link through which its information security can be circumvented.

Additionally, Cisco (2013) indicates that workers today want the freedom to browse the web beyond the when to browse and the how to browse. They want the freedom of choosing which devices they browse with. However, they don't want these freedoms and their privacy invaded upon by their employers. These users do not agree with employers tracking the employees' online activities even on company-issued devices. They believe that employers have no business monitoring such behaviours. Where this is the case it poses a challenge to information security personnel. If there is no record of both successful attacks and attempted attacks, it might be difficult to choose the right security technique that can secure an organization's information resource. If an organization has no idea who its enemies are, it becomes difficult to know what security measures to put in place in order to prevent future break-ins. Without the right security techniques in place it is difficult to secure the organizations data resources as employees could easily browse sites that could put the organization in harm's way.

Furnell, Jusoh & Katsabas (2006) also state that, although some users actively seek to overcome secure configurations, the most likely scenario in most cases is the fact that security configurations are unused or configured incorrectly thereby exposing the organization to risks.

This study outlines the threats, risks and vulnerabilities associated with the use of portable devices such as smartphones by mobile workers and any other worker for that matter. The study proposes some solutions that can be adapted while using these devices as they are intended to be performance enhancement tools and cannot be eliminated from our lives. Additionally, the study analyzes the challenges that mobility brings to Information Security and how the socio-technical theory can be used to address the problems that portable devices such as the smartphone bring to organizations.

Smartphones have come to stay. Whether we admit it or not, they will be used consciously or unconsciously for work related activities. For this reason researching into its strength and weakness as work related tools is important to both organizations and users.

1.2 Problem Description

Good security is characterized by "defence-in-depth" as a strategy that helps to limit the threats associated with the use of Information and communication technological devices (McDonough, 2003). In spite of this knowledge, some organizations though adhere to this security strategy, do not close all points of risks such as the one through portable devices. The assurance and sustenance of a secure environment is a continuous interest both in defence and in civil operations.

Portable devices such as smartphones have become powerful and can support many applications that were previously only accessible on personal computers (Couture, 2010). While using portable devices, access to data that is needed for work can be provided seamlessly through mobile computing technologies (Chen & Nath, 2003). These have led to an increase in the use of the smartphone exponentially in the last 5 years (Ahmed et al., 2009; Neilson, 2010; Ruggiero & Foote, 2011; CISCO, 2013). The increase in the use of smartphones is obviously a source of unexpected interruption to corporate operation and personal confidence and as such poses a challenge to the security of vital and exclusive information. In spite of this, a large number of smartphone users are not fully aware of vulnerability issues and the challenges that their mobility coupled with their device usage pattern brings to information security in their organizations. This is a great concern for organizations especially for organizations where security is of prime significance. This also holds true for the main benefactors of this research.

Ruggiero & Foote (2011), indicate that as the sale of smartphone increases, attacks on these devices are bound to increase. Not only are old techniques useful in breaking the security of these devices, new ones are being developed every day by attackers to help them out smart smartphone users. It is not so much as to what trick they will use but rather of what the unsuspecting user does not know. Anything goes when it comes to cyber exploits today as long as the method selected will get the job done (Cisco, 2013, p. 51). A typical activity like sending a picture through MMS can be used to break a user's privacy on their mobile devices without their knowledge. Ruggiero & Foote (2011) go on to say that between 2009 and 2010,

the number of new vulnerabilities in mobile operating systems such as Android, IOS, Symbian and windows mobile reported was increased by 42%. This is an alarming figure and a cause for concern. These vulnerabilities are becoming highly sophisticated; they can change state and character to avoid being detected. Despite the alarming rate of increase, measures to help curb these vulnerabilities on smart devices do not respond to same level of growth.

According to Takesue (2007) and Ernst & Young (2012), smartphones are used by employees as working tools without them realising the dangers they may present when used to carry organizational digital assets both inside and outside the organization. As most users are deficient in this regard, cybercriminals take advantage of the rapidly expanding attack surface found in today's "any-to-any" world, where individuals are using any device to access business applications in a network environment that utilizes decentralized cloud service (Cisco, 2013). PricewaterhouseCoopers (2012) indicate that just 44% of organizations have a mobile security strategy in place. They indicate that 45% of respondents to their 2012 security survey have a security strategy to address personal devices in the workplace yet only 37% have malware protection for mobile devices. Though there seem to be some growth in the adoption of policies and safeguards in place for secure mobile communications in organizations, it still remains at a lower rate compared to how fast mobile technologies are growing (PricewaterhouseCoopers, 2012).

1.3 Purpose / Objectives

The purpose of any research is to gather evidence that is not already known (Taflinger, 1996). This study sought to find out the effects of using smartphones as working tools especially by workers whose mobility rate are high and the challenge it poses to the organization's information security. The study also sought to gather evidence that there are indeed some risks and vulnerabilities that these devices are susceptible to and analyzed the current perception of workers regarding threats to smartphones when used for work in the organization under study.

The organization under study is an educational institution. The sample was chosen because of their mobility rate both inside and outside their organization and the ease with which interviews could be done with them. This study is done on behalf of the Swedish Defence.

The objectives of this study are highlighted below;

i. Make a study of the perceived or experienced threat and negative consequence of the use of smartphones by employees to information security in an organization.
ii. Make an analysis to identify the most significant threat and risk areas of the use of smartphones within an organization.
iii. Study countermeasures that could facilitate relatively threat free working environment even with the use of smartphones.
iv. Analyze the challenges that mobility brings to Information Security.

1.4 Research Questions

The under listed questions help to achieve the purpose and objectives that have been outlined for this study:

R.Q.1: What are the threats, risks, and/or vulnerabilities associated with the use of smartphones as working tools?

R.Q.2: How can the threats, risks, and/or vulnerabilities associated with the use of smartphones as working tools be controlled in order to maximize the added functionality of their use as working tools?

R.Q.3: How does mobility challenge information security and how can the socio-technical theory be used to address the problems of information security and mobility?

1.5 Scope and Limitations

This study outlines some of the current threats, risks and vulnerabilities associated with the use of smartphones and the most significant threat and risk areas of the smartphone. It also outlines the perception of smartphone users with regards to information security. Lastly the study analyzes the effect of mobility and smartphone usage on an organization's information security. Since workers in an organization use different smartphones that run different operating systems; IOS, Android, Symbian or windows mobile; the aim of the study is not to target any particular operating system. An Operating System here refers to the software that supports the phone's functions such as calling, browsing, scheduling tasks, executing applications and controlling other devices that can be used by the smartphone such as Bluetooth devices and head sets, etc. Any phone that meets the specifications for a smartphone as described below will be used for this research. The smartphones in question are those that have support for document reading, portable media players, low-end compact

digital cameras, pocket video cameras, touch screens, web browsers, GPS, Wi-Fi, Mobile Broadband, ubiquitous connectivity and runs on an operating system such as the android operating system, IOS, windows or Symbian. The smartphones to be used for this research are those that are bought by an organization for employee's use or the ones that the employees own themselves.

This study has several limitations that may affect its transferability. The study was limited to one section of the Computer Science, Electrical and Space Engineering department of a University. The number of respondents was seven (7) made up of researchers and lecturers. Their experiences and attitudes cannot represent all the possible scenarios of using the smartphone for work especially due to the fact that the organization in question is not one that produces so much confidential data. The research site used in the research may not represent the conditions for other mobile workers in other sites.

1.6 Significance of Study

The significance of this study is to outline the challenges that employee mobility and the use of smartphones for work pose on information security. This will help determine appropriate ways of using smartphones that will yield maximum productivity when used as working tools and minimize the threats that would be identified.

Smartphones offer many advantages in increased productivity and ubiquitous availability of personal, client and corporate data (Couture, 2010). With the help of smartphones mobile workers are able to stay connected to their clients and co-workers. By the use of this tool, they are able to respond to work related emails while away from the office, conference meetings via Skype and other apps and sometimes able to connect their laptops through this device in areas where their laptops cannot have internet access so as to be able to work.

As part of determining the threats, vulnerabilities and risks associated with using smartphones as working tools, this study proposes some solutions to help minimize the problems that are identified to the barest minimum and sheds some light on the challenges that mobility poses to information security. Finally the report suggests ways of using the social technical theory to help solve some of the problems identified.

This research can serve as reference material for further research and help organizations that rely heavily on smartphones for business to put in measures that can help to curb the risks involved with their usage as working tools.

1.7 Organization of Thesis

This thesis report is made up of seven chapters. The first chapter herein introduces the research area with some background information and other information giving the pedagogic description of the research process. This serves as foundation for understanding the relevance of the research and also helps to put it in a contextual perspective.

Chapter two is a theoretical background of the thesis. It gives a detailed review of the state of the art on information security and threats and vulnerabilities associated with the usage of smartphones as working tools.

Chapter three introduces the theoretical framework for this research. It looks into mobility as a concept and how it helps to analyze the problems of using the smartphone as a working tool and lastly uses the socio-technical theory to place the smartphone in its rightful place.

Chapter four presents the literary study, the interview process and the data analysis done in this study. Chapter five presents the Empirical findings made in this study and answers the research questions R.Q.1 and R.Q.2. Chapter six presents the discussion based on findings done in this study and answers the research questions R.Q.3.

Lastly, chapter seven concludes the research and presents some future work that can be done in this research area.

CHAPTER TWO

THEORETICAL BACKGROUND

This chapter provides a theoretical background into information security and smartphones. It highlights the importance of information to any organization and presents the smartphone as a tool that can improve the effectiveness and efficiency of work. It highlights the need for organizational information security and the pressure that management and employees put on security components as they attempt to maximise efficiency and minimise workload. Some threats, risks and vulnerabilities associated with smartphone as working tools are also elaborated upon.

2.1 Organisational Information Security

A variety of research work has been done regarding the use of smartphones as complements to the already available IT infrastructure. Several researchers have tried to find out ways by which this device can be used without increasing the risks associated with their usage (Basole, 2008; Beurer-Zuellig & Meckel, 2008; Allam, 2009 ; Ahmed et al., 2009; Botha et al., 2009; Büscher & Urry 2009; Ernst & Young, 2011; Fitzgerald, 2009; Cisco, 2013 and PricewaterhouseCoopers 2013). Though some researchers tried to analyze problems associated with smartphones usage as working tools through the socio-technical theory (Kisling, 2006; Chen & Nath, 2008), not much has been done with regards to socio-technical theory as a social theory under mobilities theory.

The concept of mobile work has received increasing research interest in recent years. However, there seem to be little work done on creating a comprehensive framework that incorporates key issues related to corporate support for mobile workers. Creating an effective mobile work environment must take into consideration not only the technical issues but also the social and cultural issues in and out of organizations as security is purported to be the number one obstacle for mobile workers, and is weighed much higher than other concerns such as cost and complexity of mobile data solutions (Ernest-Jones, 2006).

Global markets and business operations are possible through technology. Organizations make business deals, hold meetings, schedule appointments, track client account, inventory company assets and coordinate businesses all over the world from a single location by means of information technology (Whitman & Mattord, 2004). Organizations strive to meet the

demands of their clients from different locations with the help of information technology. For an organization to be competitive and remain in business not only must the organization depend on the use of information technology, it must provide a means through which it can secure information that is transferred from one end to another whether from a client to the organization or from an employee to another employee within and outside the organization. It must seek to protect information transferred from computer to computer as well as information transferred via portable devices such as smartphones.

Though employers and employees are embracing the numerous functionalities offered by portable devices such as tablets and smartphones, they are not equally aware of the information security risks associated with the use of these devices to the organization (Furnell et al., 2006; Takesue, 2007; Botha et al., 2009; Allam, 2011).

The survival of an organization depends on its ability to continuously protect the information it generates from time to time so that their clients can continuously enjoy the confidentiality, availability and integrity of transactions with the organization.

2.2 Information as an Asset

An organization's information asset whether tangible or intangible is one of the most important assets the organization owns. Musaji (2006) indicates that information assets include and are not limited to systems, data, images, text and voice and are contained within the internal systems that support the company's business activities. Though information assets are important to organizations, its value to the organization is not always quantified as it does not appear on the balance sheet of the organization (Moody and Walsh, 1999; Allam, 2009). Information is one of the overlooked assets which seem to suffer from neglect. The value of an organization's information cannot be over emphasized as it stands to be one of the key players in boosting an organization's competitiveness.

Effective implementation of information security strategies for informational assets in today's organization still remains a daunting task (Ernst & Young, 2011; Fratto, 2009; TechAmerica, 2012; PricewaterhouseCoopers, 2012; Allam, 2009). This may be primarily attributed to the fact that it involves securing data at rest, data in transit and the data used in transactions as well as other equipments that facilitate the storage of data and its movement (Allam, 2009; Whitman & Mattord, 2011). Additionally, it could be attributed to the fact that the rules of

optimal security keeps changing. Both the organization and the cyber criminal are armed with adept technological skills thereby increasing the risks to a higher point than ever before as there is no way of telling what your opponent knows or has that you don't (PricewaterhouseCoopers, 2012; Fratto, 2009).

Organizations often spend huge amounts of money and time on implementing technical solutions, but somehow wholly or partially neglect the human factor in information security (Kruger and Kearny, 2008; Dhillon & Backhouse, 2000). They forget that whatever technical solution they implement must be used by humans and as such the human aspect must also be taken into consideration. For technical system to be effective, the social system must also be effective (Kisling, 2006, p. 76). Employees to some extent determine if technological implementations will work or not. No matter how good technical controls are if employees refuse to work with them but rather use other means of working that makes things easy for them neglecting security, the objective of security would have failed. Linking human activities to security issues by involving humans in information security implementations is as important as any technology that is implemented (Kruger and Kearny, 2008) in order to minimize resistance. Technical controls are important in securing information as there is the need to safeguard who accesses which computer systems and what they can and cannot do once admitted (Dhillon & Backhouse, 2000). If people are to be involved in information security implementations then, information security ceases to be just a technical problem but also a social and organizational problem which can be minimized with the right mix of social theory, organizational theory and management science (Dhillon & Backhouse, 2000). Protecting information is not just the responsibility of management and a few employees at the technical level. It is the collective responsibility of all employees starting from the top.

With the right attitude of employees in the security of all assets including information assets, with policies, standards and procedures, and with the right education and training the value of information can be brought to light while securing it. Ensuring that information maintains its confidentiality, availability and integrity is of prime importance in information security.

2.3 Importance of Information Security and Information Assurance

Security encompasses all the activities that ensure the quality or state of being secure thereby giving an assurance of freedom from danger. As James Anderson, Vice President of

Information Security, Inovant, the world's largest commercial processor of financial payment transactions puts it, information security in today's enterprise is a

"*Well-informed sense of assurance that the information risks and controls are in balance*."

For this reason, Information security deals with the protection of information and its critical elements, and all the systems and hardware that use, store and transmit that information through technological implementations, education and training and policies and procedures (Whitman & Mattord, 2004; Maconachy, 2001).

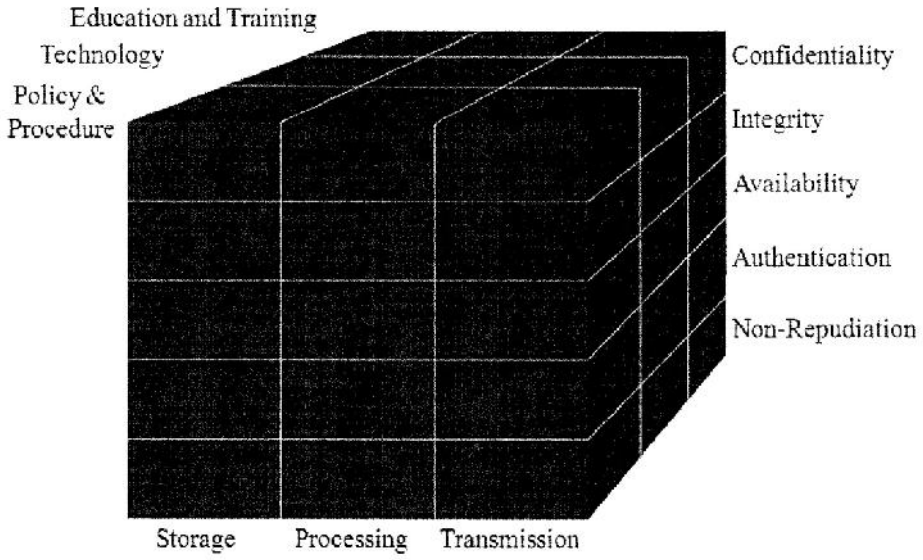

Figure 1. Extended McCumber Model (Maconachy, 2001)

As indicated in Figure 1, the extended McCumber model is a planning model of information assurance consisting of three dimensions. The x-axis represents possible states of data: data in storage, data being processed or data in transmission. The y-axis represents security services an organization can provide: confidentiality, integrity, availability, authentication and non-repudiation. The z-axis represents categories of counter measures that can be applied: education and training, technology and policy and procedure so as to achieve the security services mentioned above. This model recognizes that data could be in three (3) states; Storage, Processing or Transmission. It also recognizes that for information assurance to be fully achieved, confidentiality, integrity, availability, authentication and non-repudiation must

have been achieved. In order to maximize the benefits of information assurance, this model makes use of education and training, technology and policy and procedure.

Information security is important to organizations in order to protect the organization's ability to function, enable safe operation of applications implemented on the organizations IT systems, protect information the organization collects and uses and lastly safeguard the technological assets in use (Whitman & Mattord, 2011). Information security is also important in ensuring that an organization's intellectual property is safeguarded against theft and misuse. If an organization's information is stolen or lost, it could result in huge fines which could lead the organization to bankruptcy. It could also cause the organization to lose its integrity and reputation with its clients which may eventually lead to the collapse of the organization as clients will refrain from doing business with them (Allam, 2009).

Information Security is necessary as the threats that information technological devices are susceptible to are growing complex and ambitious with technological advancement (Standards South Africa, 2005). These threats can emanate internally or externally and can be intentional or accidental (Kritzinger and Smith, 2008; Whitman & Mattord, 2011) with internal threats in the lead (TechAmerica, 2012). Human error often leads to data breaches. Between January 2005 and June 2008, Liginlal, Sim & Khansa (2009) reported that "human error" accounted for a large percentage of internal threats identified. Allam (2009) suggests that human error accounts for most threats in smaller organisations that traditionally operate under the notion of absolute trust in employees; a trust which presupposes that employees always act within the best interest of the company. He further states that because some employers think that their employees will work in the best interest of the organization, they invest heavily on technical information security solutions that focus solely on external threats. This leaves the organization at the mercy of internal threats such as human error and employee misconduct (Daniel, 2008). Cisco (2013) also points out that because there is the general notion that good behaviour leads to good outcomes, organizations think that their information security activities are effective because they have good behavioural policies in place when in actual sense confidence in this area has diminished over the years. The truth stands out that addressing both internal and external threats with the help of policies, procedures, software and devices that work together to provide a secure and adaptive system are as important as any other objective of the organization as no one can guarantee where an

attack can emanate from. As Thomas Reid wrote in "*Essays on the Intellectual Powers of Man"*, in 1786;

> *"In every chain of reasoning, the evidence of the last conclusion can be no greater than that of the weakest link of the chain, whatever may be the strength of the rest."*

This is also true in the field of information security; a chain is only as strong as its weakest link. If organizations focus on only external threats while forgoing internal threats then no matter how strong their external security is, if internal threats can compromise the whole system, the whole system is weak. This is the reason why as part of the overall organizational security, portable devices such as smartphones must also be secured in order that they do not provide a means by which the whole organization's security and eventually information security can be circumvented.

2.4 Key Characteristics of Information Security

Information security is composed of three desirable characteristics; that is the provision of confidentiality, availability and integrity to information and information assets (Whitman & Mattord, 2004). All three components help to achieve optimal information security and are sometimes referred to as the CIA triad as shown in figure 2.

Figure 2. The CIA Triad (GFI, 2009)

Unlike traditional computer networks that are built solely on computers, networks built on both computers and portable devices such as smartphones have the tendency of needing to allow users of these devices access information resources via the network internally or

externally. Unfortunately, smartphone security is still in its infancy and so can cause a lot of problems if not handled with caution (Allam, 2009; Couture, 2010).

Confidentiality primarily restricts access to information to only authorized and authenticated persons (Whitman & Mattord, 2011). Authenticated persons are persons permitted to access the organisations information systems while authorised persons are authenticated persons with permission to access the information contained within these systems. Confidentially becomes an issue with smartphone security because of their mobility and the ubiquitous connectivity they posses. They are able to connect to both secure and insecure networks, through which they have access to organizational resources. Allam (2009) indicates that confirming the identity of a smartphone user connecting from an independent service provider requires an in-depth security approach. He goes on to say that in order to properly secure all information resources, confidentiality measures must be put in place across all mediums of information storage, communication and processing so that unauthorized and unauthenticated persons do not get access to confidential information. If this is not done, the integrity of information and information resources could be compromised. Fratto (2009, p. 18) additionally states that the concern about loss of confidential information is overwhelming especially when you consider that the term "confidential information" covers a wide swath of data, including intellectual property, the loss of which can devastate any organization.

Integrity on the other hand is a characteristic of information which seeks to promote accurate, authentic and trustworthy information by ensuring that information is whole, complete and uncorrupted (Whitman & Mattord, 2011). Information technology has made it easy to modify information. Undesired modification of information destroys the authenticity of any information thereby making that information lose its integrity. For this reason, preventing the undesired modification of information is important as it helps to a large extent preserve the integrity of information.

To provide competitive advantage, Information must be maintained in the format that is best suited to the business context that it supports. Integrity can be achieved with the help of confidentiality, yet ensuring integrity through confidentiality is not easy. Smartphones often communicate information on untrustworthy network channels. Organizations do not have control over these channels and as such ensuring the integrity of the information received and sent on these networks is important in achieving adequate information security (Allam, 2009)

Availability of information is the ability to access information when it is required (Whitman & Mattord, 2004). Availability, if adequately addressed, can provide competitive advantage for employers. While using smartphones as working tools, organizations must make extensive use of untrustworthy networks. Adequate security for an organization's information should provide mitigation strategies for untrustworthy communication channels as restricting access to untrustworthy networks could reduce or halt productivity gains possible through the use of smartphones (Allam, 2009). Appropriate levels of confidentiality, integrity and availability must be used in order to maximize productivity while improving information security.

2.5 Creating an Information Security Culture

An Information Security culture emerges from the way in which people behave towards information and the security thereof (Ghonaimy, El-Hadidi & Aslan, 2002). It also encompasses all socio-cultural measures that support technical security measures, so that information security becomes a natural aspect in the daily activities of every employee (Schlienger & Teufel, 2003). This makes taking into consideration the organizational culture of an organization important when implementing information security (Connolly, 2000). This is because the information security system as Chia, Maynard and Ruighaver (2003) identified is one system that is supported by management's beliefs and actions.

Businesses depend on their information assets for survival. In as much as technical information security solutions are good, they are not enough to help secure these information assets. Dhillon (2001) suggests that, the effectiveness of information security controls depends on the competency and dependability of the people who are implementing and using it. For this reason, one of the most important aspects of an effective information security programme is employee awareness (Olzak, 2006).

Organizations must incorporate security awareness programs into their activities from the time an employee is hired and throughout the lifetime of the employee through direct and indirect means (Whitman & Mattord, 2011; Allam, 2009). The use of technical solutions such as the implementation of firewalls and gateways can go a long way in securing the organization from external threats but if they are not implemented well, if users do not know how to use them or if they are not maintained well the whole information security approach could become vulnerable to both internal and external threats. This would eventually create a

culture where security is implemented in a haphazard manner and a culture where employees disregard any form of secured means of work.

Schlienger and Teufel (2002) additionally suggest that during recruitment, employees must thoroughly screen prospective candidates with considerations to individual privacy and the data protection law before employing them. They argue that doing this can help improve security of the organization greatly and prevent unmotivated and malicious staff from being employed. They go on to say that a thorough screening of prospective employees will help the organization to choose highly motivated and qualified staff which will in the long run help to decrease external threats through email viruses and worms.

Policies, procedures and standards that organizations use in achieving their organizational information security must consider the organizational culture in order that changes and improvements made to existing information security procedures are not met with defiance by employees.

2.5.1 Security Awareness Culture

Martins and Eloff (2001; p. 1) state that:

> *The way in which people interact with information assets and how they behave in the working environment will in time become the way in which things are done in the organization.*

The processes and procedures defined at the organisational level, together with the guidance of managers and other influential individuals, shape the attitudes of employees (Martins & Eloff, 2001). This eventually becomes the culture of the organization. People who don't know how to do things rarely do them well (PricewaterhouseCoopers, 2012, p. 23). Security programs cannot be effective without adequate training (Whitman & Mattord, 2011; PricewaterhouseCoopers, 2012). There is the need therefore for individuals to be enabled and equipped to form a culture of information security through awareness and training.

Most security breaches occur because trusted internal employees of an organization subvert existing controls (Dhillon, 2001). Ruighaver et al. (2007) indicate that there is no evidence that employees are naturally motivated to adopt secure practices of working. The only way to

get employees to desist from misconduct is to incorporate learning about the importance, usefulness and necessity of security controls, in order to discourage them from attempting to bypass these controls. This can be achieved through employee motivation and rewards such as money and recognition (Allam, 2009).

Organizations must be concerned about capturing the minds and hearts of their employees and getting them to work as the policies in place suggest they should in order to reduce resistance (Hughes & Stanton, 2006) and create a culture where information security is not circumvented (Allam, 2009). If policies written are not enforced and employees work in ways to put the organization at risk, it will soon become how they will work. New employees that join the organization will also learn to work in the wrong way as that would be the organizational culture that every employee is welcomed into.

A healthy organizational culture will assist in promoting almost any productivity level that senior management requires (Allam, 2009). If employees understand the risks involved in using smartphones for work and know how to use it in order to minimize these risks, obviously productivity levels will increase. Especially for workers who are highly mobile and need to respond to emails or access organizational information via their smartphones every now and then while on the move.

2.6 The Information Workforce

Not all information that an organization owns is explicit. Some information is tacit. It resides in the minds of employees. As Allam (2009; 50) puts it,

> *People are the ultimate source and destination of the information found within organizations.*

Information by itself without people using it for the maximum benefit yields almost nothing as it cannot work on itself to yield any benefit. For this reason organizations must recognize that the modern workforce is fuelled by information.

Information security though protects an organization's information by way of enforcing confidentiality, integrity and availability should not in any way prevent employees from their daily tasks while at work or put additional stress on the working procedures of employees.

There should be a balance between protecting information, and enabling authorised access (Post & Kagan, 2007). Restricting access to information should be done with careful consideration and with emphasis on security and accessibility by authorized and validated users (Whitman & Mattord, 2011). Tightening security by making systems inaccessible can discourage employees from working and eventually make them less productive. Thus striking this balance becomes vital to the success of any information security solution.

Mahoney (2009) states that the adoption of new technologies is rapidly increasing with the proliferation of workers who view technology as a way to make business processes more effective, flexible and mobile, while increasing collaboration. This can be seen from today's world where portable devices such as smartphones have been incorporated into the daily activities of our lives. Mobile workers are usually dependent on this technological device to continuously provide the services that they are required to provide as seamlessly as possible through various networks both trusted and untrusted. This flexibility poses a great risk as employees connect through different information super-highways that are not managed by their organizations. This gives hackers, viruses and spyware the opportunity to exploit an organization's resource if they do not manage very well how their employees connect from outside networks.

2.7 Effects of Information Security on Organization Behaviour

If employees understand the need for security, then it is very likely that they will accept it. On the other hand, if they do not understand the need for information security, then they may not accept it. If policies prevent employees from working, if policies make their work cumbersome, they may circumvent these policies and work in ways that will make them efficient thereby disregarding information security and putting the organization in one risk or another. It is for this reason that Hughes and Stanton (2006) emphasize the need for organizations to win the hearts and minds of their employees so that policies that they formulate will be adopted by these employees. They explain that winning the minds and hearts of the employees involve more than educating them on the policies set. They suggest that it requires making employees and users understand the importance of what is being put in place and the reason behind it being put it in place. This they say will prevent the notion by Furnell and Thomson (2009) that people are often perceived as an obstacle rather than an asset to information security efforts. Hughes and Stanton (2006) explain that Winning the minds and hearts of employees in information security policy implementations must be a

constant approach used by organizations to capture the attention of their employees if they want to stay on top. This is because as information technology improves, threats will become complicated thereby forcing organizations to change policies and create new ones that will support the organization. If they don't make it a habit of getting their employees on board, they may force these employees to look for simpler ways of performing their tasks. This will not only cause the organization to suffer some risks but will also make the organization's goal of providing information security unachievable.

Additionally, organizations must be clear through policy what measures are in place to protect organizational information. Not only must there be policies that support organizational information security, employees must be educated and made aware of these policies so that they can incorporate them in their work in order that the goal set out by these policies will be achieved. They must also be made aware of punitive measures in place for those who defy these policies. This will make it easy for employees to accept the policies thereby reducing resistance to information security policies.

2.8 Smartphones Risks

Whitman and Mattord (2004) define a risk as a product of the likelihood of a vulnerability to be exploited and the impact of a threat against the information assets of an organization or an individual. Threats exploit one or more vulnerabilities. The likelihood of a threat is determined by the number of underlying vulnerabilities, the relative ease with which they can be exploited and the attractiveness for an attacker.

Chinese general Sun Tzu, in a publication "*The Art of War*" is quoted as saying;

> "*If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle*"

Knowing what risks, vulnerabilities and threats exist in using the smartphone as working tools will help come out with appropriate mechanisms to control or limit the negative consequences of using the smartphone as working tools. When risks are successfully exploited, there could be a loss in one or all of the following to organizations and to users of the smartphone;

personal data, corporate intellectual property, classified information, financial assets, device and service availability and functionality and a loss in personal, political or organizational reputation. Below is a summary of the top ten smartphone security risks as compiled by Enisa in December, 2010.

No.	TITLE	RISK	DESCRIPTION
1	Data leakage resulting from loss of device or theft	High	Occurs when the smartphone is stolen or lost and its memory or removable media is unencrypted, allowing an attacker access to the data stored on it.
2	Unintentional disclosure of data	High	Occurs when the smartphone user unintentionally discloses data on the smartphone.
3	Decommissioned smartphones attacks	High	Occurs when the smartphone is decommissioned improperly allowing an attacker access to the data on the device.
4	Phishing attacks	Medium	Occurs when an attacker collects user credentials (such as passwords and credit card numbers) by means of fake apps, through SMS or email messages that seem genuine on the smartphone.
5	Spyware attacks	Medium	Occurs when the smartphone has spyware installed, allowing an attacker to access or infer personal data. Spyware covers untargeted collection of personal information as opposed to targeted surveillance.
6	Network Spoofing Attacks	Medium	Occurs when an attacker deploys a rogue network access point either through Wi-Fi or GSM and the unsuspecting user connects to it. The attacker subsequently intercepts or tampers with the user communication to carry out further attacks such as phishing.
7	Surveillance attacks	Medium	Occurs when an attacker keeps a specific user under surveillance through the target user's smartphone.
8	Dialler ware attacks	Medium	Occurs when an attacker steals money from the user by means of malware that makes hidden use of premium SMS services or numbers.
9	Financial malware attacks	Medium	Occurs when the smartphone is infected with malware specifically designed for stealing credit card numbers, online banking credentials or subverting online banking or ecommerce transactions.
10	Network congestion	Low	Occurs when the network resource is overloaded due to smartphone usage leading to network unavailability for the end-user.

Table 1. Top Ten Smartphone Security Risks (Enisa, 2010)

2.8.1 The Smartphones

A smartphone is a large-screen, voice-centric handheld device designed to offer complete phone functions while simultaneously functioning as a personal digital assistant (Gartner, 2009). Palm also defines a smartphone as a portable device that combines a wireless phone, e-mail and Internet access and an organiser into a single, integrated piece of hardware (Elgan, 2007). Both definitions provide a reasonable description of the operational facilities provided by the smartphone. Below is a picture of how the smartphone looks.

Figure 3. Sample SmartPhones (Verge Staff, 2012)

Defining a device as a smartphone or regular mobile phone is not an easy one to do. For this reason this review does not wish to provide a definitive definition for what exactly a smartphone is. It considers though a smartphone as one with the capabilities stated in the two definitions above and additionally that have support for document reading, portable media players, low-end compact digital cameras, pocket video cameras, touch screens, web browsers, GPS, Wi-Fi, mobile broadband and ubiquitous connectivity. For a phone to be considered truly as a smartphone it must have all the capabilities as stated above.

Because smartphones provide document reading capabilities, are able to process, store and transport information, they are used by workers as working tools (Allam, 2009). Reardon (2007) predicted that between 2007 and 2012, there was going to be more than a 30% year-on-year growth in the sale of smartphone. Smartphones have become a common portable device owned by employees due to its rapidly decreasing unit prices (Allam, 2009). The ease with which employees can now own smartphones coupled with the fact that it has similar

capabilities as desktop computers make them an important device in the lives of employees and as such cannot be over looked.

2.8.2 Smartphone Vulnerabilities

Whitman and Mattord (2004) define vulnerability from the information security perspective as an identified weakness of a controlled system in which necessary controls are not present or are no longer effective.

In the past, organizational information security was mainly only concerned with devices that were physically connected to the network of the organization, or within the organization's physical perimeter (Allam, 2009). Though this seemed to have worked for organizations in the past, there is now the need to secure portable devices that have wireless connections. The use of portable devices including smartphones have introduced the need for wireless security, which according to Stanley (2004), is inherently less secure than their wired counterparts. Smartphones vulnerabilities differ from traditional computer security vulnerabilities. Most organizations already have a mechanism in place to manage desktop and laptop security related problems (Hunter, 2008).

Unlike desktop security, smartphone security is still in its infancy and as such involves a lot of considerations to be made if they are to be used as compliments to the already existing devices used on the networks. Now more than ever it is important that smartphones are managed just as computers on the network are managed.

The increase in the use of smartphones as a result of the decrease in unit cost and its ability to support applications that were previously only accessible on computers has caused an unexpected interruption to corporate operation and personal confidence. The nature of some employee's work demands that they move about from client to client while performing their task. Workforce mobility has necessitated the need for smartphones as the device helps these workers to connect to their organizations and to their clients seamlessly. This poses a challenge to the security of vital and exclusive information.

Smartphones support ample storage capacities. Not only do the devices have big storage spaces, the spaces can be extended to provide even more space (Johnson, 2009). As a result it enables employees to store large amounts of organizational information on them. This

information forms part of the organizations information asset. The reality is that the information that is stored on these phones is worth more than the value of the smartphones they are stored on (Allam, 2009). For this reason protecting the smartphones used by employees has become necessary for the survival of these organizations.

Smartphones vulnerabilities can be addressed from expandable storage, physical threats, configuration and users, authentication, communication and applications as outlined by Botha et al. (2009) and Landman (2010).

2.8.2.1 Expandable Storage

Expanding the memory capabilities of a smartphone is by itself not a bad thing to do. However, very often these cards are not encrypted. Even in situations where there is an option to encrypt external memory, a larger percentage of users leave them unencrypted perhaps due to the fact that they are not aware that this can be done, they do not know how to do it, feel it's too much work for them to do or do it but incorrectly as Furnell et al (2006) suggest. Accessing the information on an external memory in most cases does not require separate authentication. This means that if the phone is lost or stolen, and the memory card falls into another person's hand, the information on the external memory can be read from other devices with little ease even if the phones are blocked and unusable. This introduces an element of risk, should the device, stick or card fall into the wrong hands. Botha et al. (2009), state that a malicious user would be able to insert unencrypted expansion media from one device into another device in order to easily access that information.

2.8.2.2 Physical Threats

Due to the fact that smartphones are mobile and portable, they are more likely to be exposed to destructive elements such as sand, water or fire than fixed machines which may be under several levels of protection (Allam, 2009). Both Botha et al. (2009) and Heikkila (2007) indicate that smartphones are more vulnerable to physical threats such as theft and accidental loss, than larger systems in fixed locations. According to Banks (2010), as many as 31,544 smartphones were left in New York City taxis within a period of 6 months. Additionally Landman (2010) reports that in 2005, a survey of taxi drivers in London and other cities by Pointsec and the Licensed Taxi Drivers Association reported over 60,000 mobile phones along with 5,500 PDAs and 4,500 laptops left in their cabs over a six month period. This suggests that loss of smartphones is very likely to happen and happen on a daily basis. Such a

loss can result in financial damage for organizations than malware attacks. Smartphones are also prone to the risk of improper disposal. Ernest-Jones (2006) reports an incident involving a Wall Street banker who sold his supposedly non-functioning Blackberry upon leaving his employer resulting in the buyer getting hundreds of private emails and a huge detailed contact list after putting in new batteries.

If organizations are to use smartphones as complements to the already existing IT infrastructure, then they must make room for the protection of smartphones in their information security risk management techniques. Information stored on smartphones must to a large extent be controlled so that customer data, organizational information and trade secrets, etc do not fall into the wrong hand when the phone is lost or stolen.

2.8.2.3 Configuration and Users

Unlike computers used inside the confines of an organization, smartphones though are used by employees for working purposes are in most cases privately owned. Even when organizations bought them for the employee, they are managed by the employee and not by the organizations in which these employees work. The security configuration of this device is left in the hands of the owners of these phones to suite their preferences. As a result smartphone security has become a point of neglect by most organizations (Botha et al., 2009). Landman (2010) suggests that a great deal of vulnerabilities caused through the use of smartphones in work places is as a result of employee behaviour. The careless nature of some employees, the fact that some employees are unaware of policy or the deliberate attempt to violate policy by some employees can cause a lot of risks for organizations whose service delivery depends on a great deal of smartphone usage. Not all users possess the technical knowhow of how to securely configure their smartphones to support the organizations information security needs. Some users will actively seek to overcome secure configurations, whereas the most likely scenario is that security configurations will be unused or configured incorrectly thereby exposing the organization to risks (Furnell et al., 2006).

Activities such as employees turning off security applications such as antivirus software or firewalls, downloading infected applications consciously or unconsciously from the web, using instant messaging or file sharing software in violation of policy, putting confidential information on removable storage devices, and putting confidential information in emails sent

to unauthorized recipients could cause the organizations information security to be circumvented. Smartphones make it easy for any of these activities to be performed.

One problem with employees or users is that not all of them are trustworthy. This in itself can be a form of potential threat. Landman (2010) indicates that disgruntled employees out for revenge, former employees sharing confidential information with a future employer or an individual selling confidential information for personal profit could be disguised as a trustworthy employee within an organization.

2.8.2.4 Authentication

Botha et al. (2009) indicate that smartphone users are against periodic re-authentication and consider it to be intolerable on smartphone devices. Though these users do not have any problem with putting a password on their desktop machines, they fail to do same on their smartphones as they consider it to slow them down while using the device. Jürjens, Schrek and Bartmann (2008) say that users tend to have a short and nomadic usage pattern with smartphones, leading to reduced acceptance of full-blown security checks for relatively low and spontaneous uses.

Clark and Furnell (2007) also add that existing PIN-based techniques are under-utilised, and provide an inadequate level of protection when compared to the sensitivity of data and services accessible through these devices. Smartphones are usually used to perform a limited set of tasks in an equally limited period. In contrast, major undertakings are performed on the desktop machine over extended periods. Therefore, users tend to configure their smartphone device to deliberately avoid periodic re-authentication for the sake of convenience (Allam, 2009).

Landman (2010) states that most users assume that the authentication protection provided by the Personal Identification Number (PIN), on their smartphones will protect them whereas this is not always the case. He makes mention of a scenario where IT blogger Jim Mareinfeldt was able to bypass the 4 digit pin in the current IOS of an iPhone, thereby accessing almost all of the data stored on the phone and getting out without leaving any sign that the phone had been hacked. He reports that even though this incident was reported to Apple, nothing had been done to correct this vulnerability as of June 7, 2010.

Landman (2010) also points out that smartphones are susceptible to direct attacks via Bluetooth. This vulnerability allows hackers to gain access to the smartphone and eventually control the smartphone. Bluebug and Bluesnarf allow the attacker access to contacts, text messages and other content without detection. Other direct attacks capture the PINs during pairing and use brute force techniques such as BT crack and btpincrack to reveal the PINs. Whereas it takes a four digit PIN a few milliseconds to crack, a sixteen digit PIN could take thousands of years to crack. This makes the choice of PIN length very important. The choice of character combination is also very important as the use of alphanumeric characters is preferred over simply using letters, especially names that the user is familiar with. Many smartphone users never change the default PINs shipped with the device. This simplifies the task of guessing PINs with specific devices. Dunning (2010) indicates that by using Car-whisperer it is easier to get hold of Bluetooth device PINs by simply trying the most common or default PINs for Bluetooth devices particularly headsets and hands free accessories.

The Bluetooth feature "Just Works" which is used to connect to a printer without authentication can also be used by the man-in-the middle to cause denial of service attacks. When the victim tries to reconnect, the attacker's device is disguised to look like both the sending device and the printer so it becomes a relay with full unencrypted access to the entire transmission (Dunning, 2010).

2.8.2.5 Communication

Smartphones are no longer limited to communication via public cellular networks alone (Allam, 2009). Smartphones possess a number of available connectivity methods which have better throughput, latency, cost and availability (Jürjens et al., 2008). The problem as Botha et al. (2009) point out is that, smartphone users must configure network connection security settings for each network that they connect to. Jürjens et al. (2008) add that the multitude of device configurations leads to various combinations depending on the set of requirements essential for the given usage scenario. This becomes a difficult task as the majority of users do not know the appropriate security settings, and will connect to the least secure network, that requires minimal configuration. These insecure channels could expose smartphone connections to Man-in-the-middle attacks. Landman (2010) reports that SMobile Systems tested the iPhone, an HTC phone running Android, an HTC phone running Windows Mobile and a Nokia phone with all phones succumbing to the man in the middle attack. Through this

attack they were able to capture important information such as user names and passwords to various websites including emails and online bank accounts.

Additionally, Landman (2010) points out that tools such as Arpspoof is able to send fake Address Resolution Protocol replies to redirect packets, SSLstrip is used to collect HTTP communications while Ettercap and Wireshark are used to sniff, intercept and log network traffic with webspy serving as a tool that enables hackers to open sniffed out web pages.

2.8.2.6 Applications

There are numerous mobile applications that are available for smartphone devices. Not only companies that provide these phones have applications that can be used on them, third party applications are also assessable to users who are interested in additional application support provided they have enough memory to support them. When it comes to third party software installations, it is usually up to users to determine if the permissions of the downloaded application will cause an infringement on the data stored on the smartphone or not. These applications can have access to the same information that users access on their desktop machines. Below is an image that shows the permissions assigned to an application that a user has opted to install.

Figure 4. Legitimate and Malicious Steamy Window Application (Ballano, 2011)

Both applications as shown in figure 4 are supposedly the same yet the app on the right has permissions to receive SMS, read and write browser history and bookmarks in addition to the basic permissions for network communication. An application such as Steamy Window in figure 4 above should not have permission to receive SMS or read and write browser permission. This is because its main function on any smartphone is to make the phone's screen appear steamy and make it look as though there is a rainy weather on the phone. It allows water drops to move when the foggy screen is wiped with the finger.

While the level of sensitivity of the data remains the same, the security level of smartphone applications is usually much lower than the desktop version of the same application (Allam, 2009). The question is how many smartphone users take time to check out the permissions that an application would have on their phone? How many users understand what these permissions mean to their privacy? How can they tell which permissions go with which applications? How can they tell if an application they have on their computer has the same security in its miniature version for phones. Botha et al. (2009), point out that the smartphone version of internet explorer, IE Mobile, has only three security options, compared to 45 on the desktop version. They also report, that the mobile version of Microsoft Word does not support some of the key security components of the desktop version. Jürjens et al. (2008), additionally point out that the provision of patches and updates such as virus signatures is difficult on mobile platforms such as smartphones than they are on computers and laptops.

In the past, the lack of sufficient computing power was perceived as a major reason why smartphones had not been attacked as much as the traditional desktop and laptop computers. Smartphones today have evolved and have similar capabilities like computers. This has made it a conducive platform for the spread of malicious apps with all sorts of intent. Users can no longer presume that apps from their app store are trustworthy. They must deliberately scrutinize these apps by checking the permissions as well as running a background check on these apps, reading the review of the app from other users and using the help of an antivirus program installed on their smartphone to check for any malicious content. The android developer can distribute their Android apps to users by publishing the app in an app marketplace, serving the apps from a website or emailing them directly to users. Android application developers can upload their applications without any check to the trustworthiness of the application. The applications are self signed by developers, without the intervention of any certification authority. This allows for uploading both good and bad applications, including cracked applications or Trojan horses and other malware to Android smartphone

users which can compromise personal data by taking over the user's device. Arthur (2011) writes that Lompolo noted Myournet had taken 21 popular free apps from the Market, injected root exploit or code into them and republished these applications as trustworthy applications in order to get unsuspecting users to install them and eventually infect their phones. What is worrisome here is that Myournet got between 50,000 and 200,000 downloads altogether in just four days. With similar events happening around Android users, the Global Threat Centre of Juniper Networks has reported a 400% increase in Android malware since 2010. These malware consist of fake windows media players which gives permission to GPS, calling phone numbers, browser history, intercepting outgoing calls, etc. There is also Geinimi a Trojan which originated from China in December 2010. This Trojan is embedded within pirated applications for Android phones. PJApps a Trojan with back door capabilities that targets Android devices also spread through compromised versions of legitimate applications. All the aforementioned are examples of apps available on unregulated third party Android marketplaces (Ballano, 2011). There is also HongTouTou which was published in two versions, HongTouTou.A and HongTouTou.B (SecurityWeek News, 2011). HongTouTou.A is said to have lured Android users to download and install the app by hiding itself in legitimate apps such as the well-known game RoboDefense. Once activated, the mobile malware connects to a network in the background, and attempts to collect data from the user’s smartphone, encrypts it and send it to a remote server. HongTouTou.B also lured the user to download and install the mobile app under the name "Dynamic Footprint Wallpaper". Similar to HongTouTou.A, after being installed and activated, it connects in the background and attempts to collect the user data, and send it to a remote server.

Help Net Security (2013) reported another malware named as “BadNews” found on Google Play, the Android app Store. This malware harvests device information such as phone numbers and handset serials from users who had it installed, and tricked them into downloading other malicious apps. In this incident even though Google had removed the apps and the accounts offering them, millions of users had already downloaded and installed them on their devices. This malware is said to have launched itself through post-launch updates months after users had installed games, dictionaries and wallpapers, of supposedly malware free apps.

2.8.3 Smartphones Risks

In general terms a risk is any situation that could make one susceptible to danger. Smartphones risks therefore are those situations which could lead an organization that embraces its use for work and especially for mobile work, prone to breaches in its information security.

Several factors as highlighted by McAfee (2007) have been attributed to the increased risk to smartphone Malware, some of which are listed below:

- A drop in the price of mobile phones, creating an increase in the number of vendors in smartphone application.
- The fact that smartphones have the tendency to store huge amounts of personal and organizational data thereby making it appealing for malware authors because of the potential financial gains from identity theft or theft of credit card information.
- The fact that smartphone hardware capabilities have increased, the operating system functionality has also increased thereby creating new opportunities for exploitation for malware authors.
- The fact that due to the current capabilities of smartphones, users have made it a preferred choice especially where there is the high tendency of users to be mobile workers.
- The fact that most of these smartphone providers make use of platforms that have free resources that interested parties can learn from thereby making it easy for hackers to learn the strengths and weaknesses of these systems and create malware that can easily attack these systems. E.g. Where people are familiar with the windows operating system, it is much easier for them to create malware for smartphones that run the windows mobile OS because of the similarities. Windows Mobile and Win32 are very similar and so it's easy for authors of win32 malware to transition to mobile malware on a windows mobile phone.

Managing smartphones used in an organization is not an easy task since the device is used both for personal and organizational purposes and are from different vendors with different configurations, which may be unknown to users and IT personnel who administer them. According to Botha et al. (2009), organizations neglect to acknowledge the fact that smartphone configurations are controlled by their users and not the network administrators

hence may or may not have the appropriate security configurations necessary to protect an organization's information resources.

The problem of smartphone risks cannot be fully addressed without considering the concept of mobilities turn since this concept deals with the large-scale movement of people, objects, capital and information across the world. The concept of mobilities makes us realize that it is not only people that move but that as these people move, they move around with information; the consequence being the implications of these movements to the people that move and the organizations that these people work for. This concept allows us to understand why workers use their smartphones to access an organization's information resources. Beurer-Zuellig and Meckel (2008) suggest that mobilization of the work-force is the reason for the demand of new mobile and wireless technologies which facilitate contact between the growing number of mobile eWorkers and organizations. Mobile workers especially are always on the run and need to work irrespective of where they are.

Unlike in traditional computing environments, smartphone users hardly understand the security requirements of the device. Allam, 2009 suggests that because of the nature of smartphones and their use, users are less tolerant of enforcing security on them. This presents a great security risk to the organization as these devices can be circumvented, causing the overall organizational security to suffer immensely. Whereas authentication on computers can be performed by a centralized network once at the beginning of the working session, authentication is done by the smartphone device several times during the day whenever the device is used. This makes it a cumbersome task and as such makes some users of the smartphone neglect it all together.

Configuring a computer is usually done by network administrators in an organization. Using network security policies, machines can be restricted so that only what the network administrator deems acceptable can be performed on the computers. Smartphones on the other hand are configured by employees who use them according to their personal preference (Botha et al., 2009). In most cases, less security configuration options are available on the mobile operating system compared to the operating systems in use on computers. This makes it difficult in achieving optimal configuration that promotes security while using the smartphones as working tools in an organization.

Computers in the organization generally communicate on trusted wired or wireless networks. These networks are configured by internal system administrators. Smartphones devices on the other hand are able to communicate regardless of their position. This makes them communicate on untrustworthy third party networks making it easy for the overall organizational security to be breached if care is not taken (Walters, 2012).

Desktop computers are not as susceptible to physical threats as smartphones are. The mobility of smartphones makes them susceptible to theft, loss and destruction elements such as water and dirt. This makes protecting smartphone devices a bit difficult as their protection is somehow dependent on the care given to them by their users (Heikkila, 2007).

Traditional applications execute on mature operating systems with more established security components (Couture, 2010). Applications are patched more frequently. Desktop machines are commonly equipped with anti-virus software and client firewalls. Desktop machines are less likely to contain removable media. This reduces the chance of information being removed from the machine. Network administrators are easily able to restrict removable media from being connected to desktop and laptop devices if required. Mobile applications are developed for operating systems that contain a subset of security components found in desktop operating systems. Most smartphone users neglect to install smartphone antivirus software. It is highly likely to find removable media such as extended memory attached to these devices. This removable media usually does not share similar security restrictions with the device itself (Allam, 2009). Media can often be removed and accessed from other devices.

Smartphones users exchange very sensitive and private information using these phones with little regard to reliability and security (Ahmed et al., 2009). Couture (2010) indicates that the threat to smartphones is not only growing in terms of raw numbers of personal users, but also in penetration into the corporate environment. If smartphones are used appropriately, with reliability and security in mind, they could improve and accelerate work processes through the timely provision of information, enhanced reachability and the simplification of coordination processes (Beurer-Zuellig & Meckel, 2008). Sacco (2007) and Takesue (2007) both suggest that the type of information stored or accessed through smartphones would have serious consequences to the organization if these devices are lost. Information that could be lost includes intellectual property, customer data and employee details. Though there are few individuals who carry this much data on their mobile devices, the increasing connectivity and

integration into corporate networks means that a vast amount of data could be at risk by virtue of the less-secure portal into corporate systems potentially created by these smart mobile devices (Couture, 2010). As DeSanctis & Poole (1994; p125) put it, advanced information technologies bring social structures, which enable and constrain interaction to the workplace. As smartphones enable eWorkers to work with ease, there is also the problem of the risks that it presents.

A white paper by Juniper Networks in 2011 indicates that there has been an increase in malware risk from the rapid proliferation of apps in application stores. This, they claim is due to the lack of security mechanisms employed by these smart devices in helping to protect smartphone users from installing malicious applications. These malware have the tendency to send short message service (SMS) messages to premium rate numbers, background call applications that rack up exorbitant long distance bills for victims, key log applications that can compromise passwords, self propagate code that infects devices and spreads to additional devices listed in the address book. The worst part is that these malware are becoming more and more sophisticated. They are able to change characteristic during propagation to avoid detection devices (Juniper Networks, 2011; Fratto, 2009). Cisco (2013) and Fratto (2009) mention that another problem is how these threats are going to present themselves; the same threats are met by different individuals but with different methods of attack one year after the other.

> *Anything goes when it comes to cyber exploits today as long as the method selected will get the job done* (Cisco, 2013, p. 51)

The 2013 Cisco Annual Security Report states that android malware is growing substantially faster than any other form of web delivered malware. In 2012 alone, android malware grew by 2577%. This they suggest could be due to the fact that android is reported to hold the majority of mobile device market share worldwide. The report goes on to say that android has a 95% incidence in smartphone web malwares. Though some schools of thought suggest that android is safe and virus free (Dunn, 2011; Hildenbrand, 2012; Michael, 2012) possibly because of its Linux based operating system, its sandbox techniques used to run applications and the fact that Android 4.2 is able to scan already installed applications for harmful behaviour upon a users acceptance, Cisco indicates that it was hit by a botnet in 2012. They warn that the future

could hold worse encounters. This is a cause for concern as users of the smartphones with the android operating system are at higher risk with regards to malware proliferation.

Juniper Networks in 2011 further indicated the prevalence of spyware attacks on smartphones. The Federal Trade Commission Staff Report defines a spyware as a diversified amount of software that aids in gathering information about a person or organization without their knowledge. A spyware may send information gathered from a user's smartphone to another entity without the consumer's consent and can assert control over a computer without the consumer's knowledge. Information gathered may include a person's Internet usage pattern, passwords, and any other information that the cyber criminal finds interesting enough to capture. Spyware has the ability to monitor a smartphone's communication allowing cyber criminals to have complete control of the device. Spyware enables an attacker to monitor SMS and Multimedia Messaging Service (MMS) messages, emails, inbound and outbound call logs, and user locations. They also have the tendency to allow an attacker to remotely listen to phone conversations. This means that if a compromised phone is used for business, they can pose a great risk to the confidentiality, integrity, and availability of corporate data (Juniper Networks, 2011).

Couture (2010) indicates that today, remote connectivity through smartphones is used for all major classes of enterprise applications which portable laptops have employed in the field for years. He makes mention of tasks such as inventory management, sales, client record management, email and voice communications which are now actively done via smartphones. Even though this is not a bad thing, mobile devices run rapidly on evolving and heterogeneous operating systems whose security has not yet been rigorously proven under the spotlight of focused hackers and security professionals. The diversity of handsets, operating systems and their configurations, installed software and service providers makes establishing a security baseline drastically more challenging than a heterogeneous operating system such as Windows/Unix desktop environment, where mature security best practices and thorough expert knowledge exists (Couture, 2010).

CHAPTER THREE
THEORETICAL FRAMEWORK

In this chapter, mobilities theory is explained since it's the foundation on which the whole work is built. Mobilities theory is a social theory and smartphones are technical artefacts. For this reason, I analyze the socio-technical theory as a theory under the mobilities theory. Mobilities theory helps to ground the idea that people travel and exchange information including organizational data while travelling. The socio-technical theory indicates that organizations are made up of people and technology coming together to create an environment for the success or failure of the organization.

The mobilities theory is used to provide a basis for the mobility of workers while the socio-technical theory is used to place the smartphone as productive tools that are important in any social system so that they are not seen as purely technical artefacts and the organization as a separate social entity. This knowledge will help position smartphones in their rightful place from a business perspective and help incorporate the most relevant parts of the surrounding context into my analysis thereby creating conditions for successful performance at the work place.

Using the mobilities theory, some challenges that smartphones and workforce mobility pose to information security are analyzed later on in section 6.1. The socio-technical theory is also used to address the problems that portable devices such as the smartphone bring to organizations in section 6.2.

3.1 Mobilities Theory

Though mobilities theory is a social science theory, it is shifting from remaining as such into other fields of study such as information systems and information security. The breaches encountered in the field of information security are somehow as a result of mobility of the devices used and the movements by these people. Hannam, Sheller & Urry (2006) define mobilities or mobilities transformation as a concept that deals with the large-scale movement of people, objects, capital and information across the world, as well as the more local processes of daily transportation, movement through public space and the travel of material things within everyday life. Cresswell (2006), Sheller and Urry (2006) and Urry (2007) also

define mobilities as a modern pattern or model in the social sciences that investigates the movement of people, ideas and objects, and the broader social implications of those movements.

Büscher and Urry (2009) by reviewing previous research highlight the effects of 'moves' on social and material realities through investigations of movement, blocked movement, potential movement, and studies of immobility, dwelling and place making. Urry (2007) states that people of different backgrounds and professions criss-cross the globe as route ways by which they intermittently encounter one another in transportation and communication hubs, searching out in real and electronic databases the next coach, message, plane, website or Wi-Fi spot. He suggests that the scale of travelling is immense and goes on to predict that by 2010 there will be at least one billion legal international arrivals each year compared to 25 million travellers in the 1950. He also stated that there would be four million air passengers each day and at any one time 360,000 passengers in flights across the world. These travellers comprise of the nomadic worker as well as the ordinary person travelling for sightseeing or any other business other than work. In addition to what Urry (2007) predicted for 2010, the International Data Corporation (IDC) also predicted there will be more than one billion mobile workers in 2011 with three quarters of all workers across the globe being mobile workers by 2012. Urry (2007) quotes Schafer and Victor (2000, p. 171) as saying that today's world citizen moves 23 billion kilometres and will move fourfold to 106 billion by 2050. The kind of massive movement as has been predicted is already taking shape. Companies such as Ernst & Young, PricewaterhouseCoopers, Deloitte and Touch, IBM, Best Buy and AT&T are examples of companies that immensely make use of mobile workers (Conlin, 2006). Not only does the ordinary person move from place to place in pursuit of a personal gain, ideas and objects, capital and information is also moved across the world and with these movements comes the challenges of the broader social implications of such movements. Urry (2007, p. 4) indicates that being physically mobile has become for both rich and poor a way of life across the globe. While people move, they also carry along different materials openly, clandestinely or inadvertently.

In spite of all these movements, Lyons & Urry (2005) suggest that people do not necessarily spend more time travelling since this appears to have remained more or less constant at around one hour or so per day, albeit with substantial variation within any society. Urry (2007) quotes (Pooley et al., 2005) as saying that people do not necessarily seem to make

more journeys; rather they travel further and faster if not more often or spend more time on the road. Most workers travel on trains, bus and other forms of transportation each day enroute to work. Even before these workers get to the office, some reply to e-mails and other work related businesses via their portable devices especially their smartphones.

The increase in movement of people has necessitated the use of faster and efficient means of human communication. Unlike in the olden days when the post and wired telephone were the major means of communication, today, people can communicate through fax, the internet fixed line phones, mobile phones and the likes. There is an increase in the use of mobile forms of communications in recent years. Problems of Information systems and information security cannot be fully addressed without analysing mobility as this concept is changing the underlying theories of Information systems and information security especially from the point of view of confidentiality, integrity and availability.

3.1.1 The Mobile Workforce

Mobile workers are defined as employees who use ICT to access remote information from their home base, workplace, in transit, and at other destinations (Kleinrock, 2001; Jacobs, 2004). These types of workers are free from the spatial and/or temporal constraints of the traditional office (Balasubramanian, Peterson & Jarvenpaa, 2002). With the help of mobile computing technologies, the gap between these workers and the information they need for work is seamless (Chen & Nath, 2003). Korn and Ferry International indicate that over 80% of business executives are continually connected through their mobile handsets. Obviously this growth of smartphone usage for work and its corresponding growth in their applications and storage of sensitive data mean perimeter security is increasingly being breached (Fitzgerald, 2009).

McDowell (2008) reports through the Economist Intelligence Unit that 40% of executives consider at least one in five of their company's workforce a mobile worker. This is evidenced by companies such as Ernst & Young, PricewaterhouseCoopers, Deloitte and Touch, IBM, Best Buy and AT&T who immensely make use of mobile workers (Conlin, 2006). Chen & Nath (2011) are of the opinion that enterprise mobility transforms how business is conducted and greatly affects the workforce and their work. Ernst & Young (2013) indicate that mobile devices are accelerating employees' ability to access data wherever and whenever they wish creating a borderless organization. Chen and Corritore (2008) add that mobile workers have a

high degree of mobility or are often away from the traditional office desk setting, or both, and have the ability to work anytime anywhere. Due to the nature of the work of these mobile workers, Chen and Corritore (2008) refer to them as nomadic workers. These workers are always on the move, meeting one client here and there and resolving issues of partners who make use of the services these organizations provide anytime anywhere. Chen and Nath (2011) suggest that because nomadic workers can work anytime anywhere, they are not only made up of those who work away from the office but also those workers who demonstrate a high level of mobility within the workplace.

Chen and Nath (2008, 2011) suggest that though mobile working is widespread today, not all organizations are able to support and manage these types of workers. Sale (2007) and Chen and Nath (2008) suggest that many organizations have not been able to reap the full benefits of their mobile workforce. Basole (2008) and Yuan et al. (2010) attribute this to the fact that there is not enough research into the issues relevant for a successful implementation of a mobile workforce. There seems to be inadequate research work on how to incorporate the technical and social environments that is conducive for mobile work (Basole, 2008; Chen & Nath, 2008; Yuan et al. 2010).

Mobile work benefits the employee by offering flexibility, convenience, increased personal empowerment and higher quality of work life (Jacobs, 2004; Chen & Nath, 2006; Drew, 2006). It also benefits the organization by offering real estate savings, improved employee productivity, enhanced customer services, quick response to inquiries, the ability to blend expertise across space, enhanced ability to recover from disasters, enhanced corporate image and employee retention and empowerment of field employees (Jacobs, 2004; McIntosh & Baron, 2005; Conlin, 2006; Drew, 2006; Chen & Nath, 2006; Scott, 2007).

In spite of the many benefits as mentioned above, mobile work poses some challenges and risks to organizations that support them. Cisco Systems revealed that a large percentage of mobile workers had not taken the necessary steps to protect their portable devices and data (VARBusiness, 2006). Problems associated with securing the data that mobile workers work with among other issues such as difficulty of supervising mobile workers, monitoring employee activities, measuring employee productivity, and ensuring task completion are associated with mobile working (Ernest-Jones, 2006; Hoang et al., 2008).

Previous works that researched into new mobile technologies were only interested in mobile technologies as drivers and enablers of organizational transformation (Chen & Nath, 2011). Kleinrock (2001), Rouse and Baba (2006) and Seybold (2008) suggest that these researches focused mainly on how technology changed ways organizations accomplished work and in so doing over-looked other benefits, both negative and positive derived from the use of these technologies. The adoption of mobile computing technologies improves access to computing resources and communication capabilities thereby giving birth to services that are transparent, integrated, convenient, and adaptive (Kleinrock, 2001). Mobile computing technologies extend work beyond the office, and provide flexibility where timing and location of work is concerned (Chen & Nath, 2008).

According to Lopez-Nicolas, Molina-Castillo & Bouwman (2008), previous research on technology acceptance adopted theories such as the Technology Acceptance Model (TAM) and the Diffusion theory in sufficiently explaining and predicting user adoption of mobile systems. These theories at that time were sufficient to explain the haziness surrounding user adoption of mobile systems but same cannot be said about our current times. The utilitarian and social values of mobile systems now dominate user adoption decisions (Chen & Nath, 2011; p. 524). Kim & Han (2009) suggest that age and gender of mobile workers have a moderating effect on adoption of mobile technologies. Though the socio-technical framework incorporates bits of technology into our social environments, mobility and the problems associated with it are not handled properly. There isn't a comprehensive mobile workforce framework that incorporates key issues from the technical, managerial, behavioural and cultural perspective (Chen & Nath, 2011).

3.2 Defining the Socio-Technical Theory

Socio-technical or sociotechnical is derived from the words "socio" and "technical". The "socio" comprises of employees, knowledge, skills, attitudes, values and needs they bring to the work environment, the reward system and authority structures that exist in an organization while the technical comprises of machines, techniques and technological devices, needed to transform inputs into outputs in a way which enhances the economic performance of an organization (Akbari & Land, 2005; Walker et al., 2008). Simply put, Trist (1981) defines a socio-technical system as a system that is made up of a human system and a non-human system. Socio-technical or sociotechnical mean the same thing and can often be used interchangeably. In spite of this, it is sometimes difficult what to call it; Sociotechnical

Theory, Sociotechnical System or Sociotechnical Systems Theory. This often leads to a loss of its precise meaning thereby making the phrase a mere catchphrase. Irrespective of what it is called as identified above, these phrases have appeared ubiquitously in ergonomics literature for quite some time. (Wilson, 2000; p. 557) refers to it as "*purposeful interacting socio-technical system*", (Woo & Vicente, 2003; p. 253) refer to it as "*complex Sociotechnical Systems*" while (Waterson, Gray & Clegg, 2002; p. 376) refer to it as "sociotechnical work systems". For the purpose of this study, I refer to it as the socio-technical theory.

The socio-technical theory is founded on two main principles (Walker et al., 2008):

- The interaction of social and technical factors which creates conditions for successful or unsuccessful system performance and
- Optimisation of either socio, or far more commonly the technical, which tends to increase not only the quantity of unpredictable, un-designed, non-linear relationships, but those relationships that are actually injurious to the system's performance.

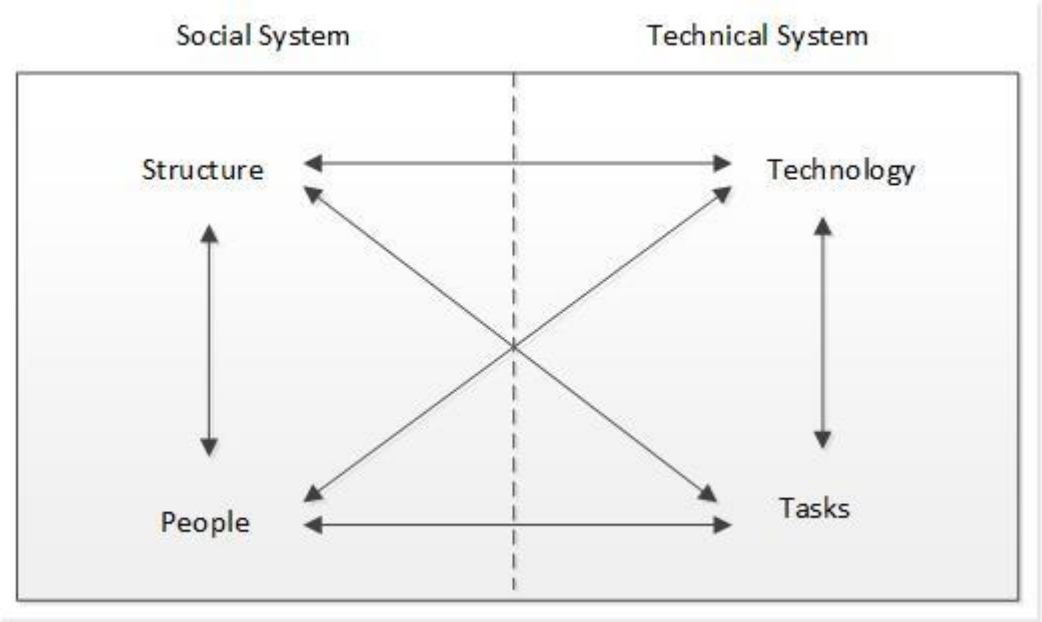

Figure 5. The socio-technical system adapted from Bostrom & Heinen (1977)

Figure 5 describes the interacting variable classes within a socio-technical system. That is; technology, tasks, structure and people. The socio-technical theory suggests that the social and technical systems should not be viewed as independent systems as the interaction and

compatibility between the technical and social systems determine the effectiveness of a work system.

Socio-technical theory reflects certain specific methods of joint optimisation that enable organisations to be designed to exhibit open systems properties that are able to cope better with environmental complexity, dynamism, new technology, and competition (Walker et al., 2008).The adoption of the socio-technical theory helps to create a fit between the technical system and the social system which together make up an organization thereby seamlessly fitting the two as one.

The smartphone is a device that can be used for social activities and at the same time for work. How can the smartphone create conditions for successful performance at the work place? The smartphone can create conditions for successful performance at the work place if organizations will use the right mix of policy, controls and education and training to administer the use of the device for work. The smartphone can erase the gap that employees and clients and/or employees and their organizations face thereby allowing them to work no matter the "where" and the "when". Mobile technologies have improved the way work and communication is done. Organizations communicate with their business partners and clients as part of their dealings. With the help of portable devices such as smartphones communication is not limited to the wired telephone or face to face communication. Workers can now chat, read important organizational documents via their smartphones and respond to important schedules no matter where they are. The socio-technical theory helps to realise that technology is essentially neutral and that failure to recognize the social system associated with the design and use of technology is the reason why many computer-based information systems fail (Bostrom & Heinen, 1977). This is why any redesign of an organization's work system must consider the impact of each subsystem on the other and meet the requirements of these two subsystems simultaneously (Rouse & Baba, 2006).

3.3 Mobile Workforce from the Socio-Technical Perspective

Socio-technical systems as already identified are made up of people and technology. Mobile workers make use of portable technological devices such as smartphones in order to work from anywhere anytime. Organizations that are heavily dependent on such devices can use the socio-technical theory as a theoretical basis to design their organizations.

Social relations as identified by Urry(2007) through his analysis on works done by Latour (1987; 1993 & 1999) shows that social relations though can be fixed or located in a place are to some degree made up of circulating or mobile entities.

The concept of mobile work has received increasing research interest in recent years (Chen & Nath, 2011; Kleinrock, 2001; Rouse & Baba, 2006; and Seybold (2008). However, there seem to be little work done on creating a comprehensive framework that incorporates key issues related to corporate support for mobile workers. Creating an effective mobile work environment must take into consideration not only the technical issues but also the social and cultural issues in and out of organizations. Security is purported to be the number one obstacle for mobile workers, much higher than other concerns such as cost and complexity of mobile data solutions (Ernest-Jones, 2006).

Identifying the key elements of both the technical and social systems relevant to mobile work makes it possible to investigate how the technical and social systems can be jointly optimized to create an environment that supports effective mobile work while suppressing the dysfunctional aspects of this work environment.

CHAPTER FOUR
RESEARCH METHODOLOGY

In order to establish a fact or a principle, a thorough investigation into a particular field of study must be made systematically and scientifically. This systematic and scientific effort is called research and can be described using the methodology and method deployed in the research process. A research methodology is the science of how research is done scientifically, emphasising on various steps that are considered in a research process to get insight or solution to a set problem along with the logic behind them (Kothari, 2009). This methodology aids in guiding the researcher towards the implementation of correct procedures to solve the problem at hand. A research method on the other hand, is the instrument that is used in performing the research operations such as experiments, interviews, tests, observation, recording data, surveys, etc. (Kothari, 2009).

This thesis is an empirical study focused on understanding the perception of users of the smartphone regarding the threats, risks and vulnerabilities that surround the use of the device, some counter measures that could help reduce these threats, risks and vulnerabilities and the challenges that mobility of the device poses to an organization's information security. The main method of gathering data was through interviews with supporting data gathered through the literature review. This study is mainly qualitative. This will help analyze data that is gathered from the target company under study and help in adequately addressing and providing solutions to the problems stated earlier in this thesis. For a thorough interpretation of what is considered under research methodology, the following are explained below;

4.1 Data Collection

Data is defined as a fact that can be communicated and stored (Spender, 1996). Data was collected through in-depth interviews which were conducted in the course of this study. Additional data was also gathered through existing research and literature. Access to this literature was through Luleå University of Technology's library resources, databases of conferences, journals, PhD thesis, technical reports and other projects related to smart phone, mobility and information security.

4.1.1 Literature Review

A systematic literature review (SLR) is used to present the previous research that has been done in the area of information security and smartphone security. SLR serves as a means of evaluating and interpreting all available research relevant to a particular research question, topic area or phenomenon of interest (Kitchenham, 2004). The review provides a balanced and objective summary that is relevant to meeting a particular need for information. In this case that need is the information on threats, risks and vulnerabilities that exist for smartphones when used in an organization as a complement to computers and the challenges that mobility brings to Information Security.

The accumulation of evidence through the literature review is valuable in offering new insights or in identifying where an issue might be made clear by additional studies. The SLR process follows three main phases as is reported by Brereton et al. (2007) each phase with sub phases;

- Plan Review
    - Specifying the Research Questions
    - Developing the Review Protocol
    - Validating Review Protocol
- Conducting The Review
    - Identifying the Relevant Research
    - Selecting the Primary Studies
    - Accessing the Study Quality
    - Extracting the Required Data
    - Synthesising the Data
- Reporting The Review
    - Writing The Report
    - Validating The Report

In addition the process of doing a literature review in information systems as is suggested by Webster and Watson (2002) was also taken into consideration.

4.1.2 Interview

This forms the qualitative aspect of the research. A qualitative interview is a type of communication between the researcher and the interviewees through conversation. Kvale (1996) suggests that when people talk to each other, they interact, get to know each other, and understand each other's experiences, feelings, expectations, and the world they live in.

In-depth interviewing is a qualitative research technique that involves conducting intensive individual interviews with a small number of respondents to explore their perspectives on a particular idea, program, or situation (Boyce & Neale, 2006; p. 3). By interviewing a sample of the population under consideration for a particular research, the researcher can enter into other people's perspectives and understand how people make sense of their world and experiences (Restine, 1999). The process of performing the in-depth interview involved;

- Planning. E.g. identifying the sample and the type of data to be gathered.
- Developing instruments. E.g. developing the rules that will guide the administration and implementation of the interviews as well as preparing the questions needed for the interview.
- Collecting the data,
- Analyzing the data. E.g. transcribing and/or reviewing the data collected through the interviews and finally
- Disseminating the findings. E.g. presenting the result of the study and discussing the findings of the study in the report.

The Interviews helped to gather vital information that helped analyze the current perception of smartphone users on how secure or insecure the use of smartphones as working tools are to their organizations and to them. Participants of the interview were asked questions geared toward finding out if they had configured their devices for optimum security, whether they were aware of the information security risks that were involved with the device usage, their mobility rate and if they were aware of any smartphone usage policies in place. The questions that were asked were open-ended. This enabled the respondent to share as much information as possible thereby enabling the researcher to gather the required information from a sample of the population under consideration. This population is a sample of lecturers and researchers

from an educational institute based of the researcher's judgement. The interview protocol is attached as appendix A.

4.1.2.1 Population and Sample

Qualitative research does not rely on traditional quantitative sampling methods which are made to ensure generalization of findings. In many of the qualitative methods, there are no strict rules for determining the minimum and appropriate number of participants to use. Instead, the research continues until the researcher is satisfied that the data yield recurrent themes and common stories (Streubert & Carpenter, 1999).

The participants chosen were those who had long standing relations with information security, easily accessible and willing to participate. These participants are lecturers and researchers. They often use smartphones as an extension to the use of the laptop as they are mobile during work both within and outside their work station.

An invitation to participate was drafted and sent via email individually to eligible members. After responding to the emails, dates for the interview were sent and participants were asked to suggest when they would be free to participate within the selected dates. Members who did not reply to the email were considered to have declined to being interviewed.

Out of the 12 emails sent on the 25th of March, 2013, 5 obliged. On the 3rd of April an email with a sample of the questions was sent to participants who had agreed to be part of the interview process so they could have an idea of what the interview was about.

During the interview two more people who were available and met the criteria of the first group emailed were interviewed.

All seven interviews were done in three days. The first two participants were interviewed on the 4th of April, 4 were interviewed on the 5th of April while the last participant was interviewed on the 8th of April. Interview times ranged from 15 minutes being the least number of minutes to 37 minutes being the highest number of minutes used. Please refer to Appendix B for Interview Schedule.

4.1.2.2 Interview Protocol

An interview protocol with an open-ended question format was used. Please refer to Appendix A for the interview protocol. The protocol had twenty-seven (27) questions that allowed me to clarify and draw expanded discussions from participants where needed. Answers to some questions meant the subsequent question did not need to be answered yet when asked; participants had stories to tell helping to get rich data for further analysis.

The first two questions were not going to be used for the study but they were asked in order to make the participant relaxed and get in the mood of being interviewed.

The major themes used for the interview are:

- Work and mobility
- General smartphone knowledge
- Smartphones security
- Applications installation and
- Policy

These themes helped to address the first and second research question and also gain an understanding of the third research question. Each interview began with the objectives of the study and the format of the interview as well as a sought permission from the participant for the interview to be recorded. This allowed me to:

- Set the tone of the interview
- Establish rapport with the participant
- Discuss the significance and format of the research
- Allow participants to ask questions before we started and
- Acknowledge the participants involvement

All interviews were done face-to-face as this I believed would help me interact better with the interviewees, and thereby help me understand their experiences, feelings, expectations, and the world they live in. This eventually helped me in presenting my findings.

4.2 Data Analysis

Data analysis helps transform the data gathered during research into useful information. The analysis begins while the data is being collected and follows through until data has been collected. As described by Corbin and Strauss (1990) and Miles and Huberman (1994) such analysis is necessary from the start because it is used to direct the next interview and observations toward sources that are more useful for addressing the research questions.

The information derived from the data analysis helps support future decision making processes. For this reason, it is a very important stage in any scientific research. As Levine (1997) puts it, data analysis is a body of methods that help to describe facts, detect patterns, develop explanations, and test hypotheses. Data drawn from interviews were analyzed in order to provide ways of discerning, examining, comparing and contrasting, and interpreting meaningful patterns or themes from the data collected. The data analysis stage of this research helped to create a variety of themes, which were later grouped into meaningful information thereby increasing the value of the new knowledge acquired.

The interviews provided an understanding of how and why respondents use their smartphones for work, what their perception is regarding the device's security, their mobility rate and the challenges that mobility brings to information security. This helped to shed more light on the reality of the mobility of these respondents and their need for portable devices such as the smartphones.

Through the examination of the first bits of information, data and cues were incorporated into subsequent interviews. Each respondent's interview was audio recorded and then transcribed to cross reference for key themes with regards to the area under study.

4.2.1 Qualitative Content Analysis

Hsieh and Shannon (2005, p.1278) define qualitative content analysis as a research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns. Mayring (2000, p.2) also define qualitative content analysis as an approach of empirical, methodological controlled analysis of texts within their context of communication, following content analytic rules and step by step models, without rash quantification while Patton (2002, p.453) suggest that any qualitative data reduction and sense-making effort that takes a volume of qualitative material

and attempts to identify core consistencies and meanings can be termed as qualitative content anaylysis.

All three definitions show that qualitative content analysis emphasizes and incorporates speech or texts and their specific contexts. Therefore, qualitative content analysis goes beyond merely counting words or extracting objective content from texts to examine meanings, themes, patterns and relationships that may be manifest or hidden in a particular text (Zhang & Wildemuth, 2009). Qualitative content analysis allowed for the understanding of social and technical reality in a subjective but scientific manner unlike in a quantitative content analysis. In table 2 the difference between qualitative content analysis and quantitative content analysis are presented.

UNIT OF ANALYSIS	QUALITATIVE CONTENT ANALYSIS	QUANTITATIVE CONTENT ANALYSIS
Research Area	Developed primarily in anthropology, qualitative sociology, and psychology, in order to explore the meanings underlying physical messages.	Used widely in mass communication as a way to count manifest textual elements, an aspect of this method that is often criticized for missing syntactical and semantic information embedded in the text (Weber, 1990)
Process of Examination	Mainly inductive, grounding the examination of topics and themes, as well as the inferences drawn from them, in the data and attempting to generate theory when necessary.	Mainly deductive, intended to test hypotheses or address questions generated from theories or previous empirical research.
Data Sampling Techniques	Samples for qualitative content analysis usually consist of purposively selected texts which can inform the research questions being investigated.	Quantitative content analysis requires that the data are selected using random sampling or other probabilistic approaches, so as to ensure the validity of statistical inference.
Product of the Approach	Qualitative approach usually produces descriptions or typologies, along with expressions from subjects reflecting how they view the social world. By this means, the perspectives of the producers of the text can be better understood by the investigator as well as the readers of the study's results (Berg, 2001).	The quantitative approach produces numbers that can be manipulated with various statistical methods.
Particular Attention to Detail	Qualitative content analysis pays attention to unique themes that illustrate the range of the meanings of the phenomenon rather than the statistical significance of the occurrence of particular texts or concepts.	Quantitative analysis deals with duration and frequency of form (Smith, 1975, p.218).

Table 2. Qualitative vs. Quantitative Content Analysis (Zhang & Wildemuth, 2009)

The use of qualitative content analysis in analysing the interviews as defined by Berelson (1952), GAO (1996), Krippendorff (1980) and Weber, (1990) allowed for a systematic, replicable technique useful in compressing many words of text into fewer content categories based on explicit rules of coding. Inductive reasoning allowed for inferences to be made by objectively and systematically identifying specified characteristics of messages gotten from the interviews (Holsti, 1969; p. 14) through careful examination and constant comparison, thereby condensing the raw data into categories or themes based on valid inference and interpretation. In order to allow for replication however, the technique can only be applied to data that are durable in nature (Stemler, 2001). The type of inductive reasoning used was conventional inductive qualitative content analysis. Table 3 gives a summary of the types of content analysis based on inductive reasoning.

TYPE OF CONTENT ANALYSIS	STUDY STARTS WITH	DESCRIPTION
Conventional Content Analysis	Observation	Helps to code categories directly and inductively from the raw data. This approach is useful for grounded theory development.
Directed Content Analysis	Theory	Initial coding starts with a theory or relevant research findings. During data analysis, the researchers immerse themselves in the data and allow themes to emerge from the data. The purpose of this approach usually is to validate or extend a conceptual framework or theory.
Summative Content Analysis	Keywords	The approach starts with the counting of words or manifests content, and then extends the analysis to include latent meanings and themes. Though this approach seems quantitative in the early stages, it helps to explore the usage of the words or indicators in an inductive manner.

Table 3. Approaches to Inductive Qualitative Content Analysis (Zhang & Wildemuth, 2009)

The choice to use the conventional analysis is due to the fact that data was gathered using open-ended questions. Interviewees were asked multiple questions to determine their perception on the security of using the smartphone for work related activities, to find out about their mobility rates while at work and whether they knew the policies that supported the smartphone that they used for work.

There were a category of techniques used for establishing relationships between the data and the unknown aspect of the problem. These methods are used for knowledge discovery from the data and for objective explanation of phenomena and patterns, which are considered to be valid, useful, novel or understandable. Below are the steps used in the content analysis.

Step 1: Prepare the Data

For a thorough content analysis, all interviews were transcribed into a separate word document for each interviewee. Later another word document was created where all the interviewee response was collated into a table with the question number as row and the individual's name as column. The corresponding cells for row and column were the answers given by the interviewees. In order to gain a deeper understanding of the answers that had been given by the interviewees, the answers were first read individually and later as a group. This helped to identify patterns, similarities and differences in answers given. Transcripts of the interviews were copied and read through consistently in order to make brief notes where Information was found to be interesting or relevant to the study. Observations, characteristics, relationships and early patterns that were gotten during the interview were also noted down and written to a separate file to help in the overall analysis later on.

Step 2: Defining the Unit of Analysis

The unit of analysis made use of themes as are listed below:

- Work and Mobility
- General Questions about the Smartphones
- Smartphones Security
- Applications and
- Policy Related Questions.

Having a unit of analysis helped ease the budden of coding as not having a unit of analysis could mean that differences in the unit definition could affect coding decisions and the comparability of outcomes with other similar studies (De Wever et al., 2006).

Step 3: Develop Categories and a Coding Scheme

The categories and coding scheme used in the content analysis were derived from the data and were done inductively. This helped to stimulate insights and to make differences between obvious categories. Constantly comparing the transcribed text helped to

- Systematically compare each text assigned to a category with each of those already assigned to that category, in order to fully understand the theoretical properties of the category; and
- Integrate categories and their properties through the development of interpretive

memos.

To ensure consistency of coding, a coding manual was developed. This manual consisted of category names, definitions or rules for assigning codes, and examples as is suggested by Weber (1990). The coding manual had an additional field for taking notes as coding proceeded. As the text was compared in the content analysis the coding manual evolved to include codes that had not been captured in the first comparisms. Table 4 shows a snippet of the code manual.

Category Name	Definition	Examples	Coding Rules
C1: Employee Mobility	To be considered a mobile worker one must be an fall under one or more of the following, • Employee who uses ICT to access remote information from their home base, workplace, in transit, and at other destinations. • Employee who is free from the spatial and/or temporal constraints of the traditional office. • Employee who have a high degree of mobility within the office or is often away from the traditional office desk setting, or both, and has the ability to work anytime anywhere.	• I travel 1 week a month. i.e. 5 days a month. 50 – 70 travels per year almost ¼ of a year, both inside Sweden and outside Sweden. • I do go for conferences and workshops 4 or 5 times a year. • During Fika, I read and respond to mails using my smartphone. I also check my schedules via my smartphone even when I'm in one meeting or the other. • I would say I have two different work places so a couple of days a week depending on the situation I am at the other office and sometimes there are travels to college meetings and conferences and these kinds of things but On a regular basis I have two offices.	All four examples point to the fact that the employee is mobile
C2: Accessing Organizational Resources	To be considered as using your smartphone for work an employee must use the device for one or more of the following, • To make and receive work related calls. • To read and reply to emails. • To save a contact list for work. • To have a schedule for work purposes. • To install apps for work. • To access other organizational resources via the internet.	• I use my smart phone only for reading and responding to emails and making and receiving calls • When I need an app for work I install it and use it. • I have a contact list on my work assigned smartphone. • I keep my work schedules using my smartphone. It's the best personal assistant I have got.	All examples indicate that the employee uses the device for work.

Table 4. Sample Codes from Data Analysis

Step 4: Testing the Coding Scheme on a Sample of Text

In order to validate for clarity and consistency of the coding scheme, a sample of the data to be analyzed was coded.

After the sample had been coded, the coding consistency was checked, through an assessment of inter-coder agreement. Coding rules were revised until the right consistency had been achieved. Doubts and problems concerning the definitions of categories, coding rules, or categorization of specific cases were discussed and resolved with the supervisor as is suggested by Schilling (2006). Coding sample text, checking coding consistency, and revising coding rules was done iteratively until sufficient coding consistency was achieved.

Step 5: Code All the Text

When sufficient consistency had been achieved, the coding rules were applied to the entire body of text. Coding was checked repeatedly during the coding process to prevent drifting into an eccentric sense of what the codes mean as is suggested by (Schilling, 2006). As coding proceeded while new data continued to be collected, new themes and concepts that emerged were added to the coding manual.

Step 6: Assessing Code Consistency

The coded data set was rechecked for consistency in coding. This step helped eliminate any inconsistencies that had been captured due to fatigue and oversight or undersight. New codes that had not been captured were also added as rechecking went on.

Step 7: Drawing Conclusions from the Coded Data

This step involved making sense of the themes or categories that were earlier on identified. Inferences were made and meanings derived from the data were incorporated into the empirical result and discussion chapter.

Activities here included exploring the categories, identifying relationships between categories, uncovering patterns, and testing categories against the full range of data as is suggested by (Bradley, 1993).

Step 8: Reporting the Methods and Findings

This is the last step in the qualitative content analysis. All analytical procedures and processes

were monitored and reported as completely and truthfully as possible as is suggested by (Patton, 2002).

The above steps were repeated severally while analysing the individual and group transcripts in order not to lose any important data. The overall process of using content analysis for the data analysis was lengthy and required that time be spent going over and over the data in order for a thorough analysis to be done.

4.2.2 Trustworthiness

In order to evaluate the trustworthiness of this study, Lincoln and Guba's (1985) four criteria for evaluating interpretive research work was used: credibility, transferability, dependability, and confirmability.

Credibility refers to the "adequate representation of the constructions of the social world under study" (Bradley, 1993, p.436). To help improve the credibility of the research results, prolonged engagement with the interview data, persistent observation, triangulation, negative case analysis, checking interpretations against raw data, and peer debriefing through several seminas were employed.

Transferability refers to the extent to which the researcher's working hypothesis can be applied to another context. In order to provide for transfereability, data sets and descriptions that are rich enough so that other researchers are able to make judgments about the findings' transferability to different settings or contexts are provided in the report.

Dependability refers to the coherence of the internal process and the way the researcher accounts for changing conditions in the phenomena (Bradley, 1993, p.437) while confirmability refers to the extent to which the characteristics of the data, as posited by the researcher, can be confirmed by others who read or review the research results (Bradley, 1993, p.437). The major technique for establishing dependability in this study is through checking the consistency of the study processes, while confirmability is determined by checking the internal coherence of the research product, that is, the data, the findings, the interpretations, and the recommendations.

CHAPTER FIVE

EMPIRICAL FINDINGS

The fundamental objective of Information security has always been to continually preserve the confidentiality, availability and integrity of information and information resources. With the advent of smart devices such as smartphones, PDA's, tablets and the likes, preserving the information security needs of an organization has become a daunting task. The smartphone is stretching the basic requirement of information security beyond the confines of an organization as was previously the case. Due to the mobility of employees and the fact that this device is handy enough to be taken anywhere and everywhere, organizations now face the challenges of providing security irrespective of where the employee is and where they use the device.

This chapter describes the findings from the study done. It provides an empirical assessment of the research questions R.Q.1 and R.Q.2 as mentioned in chapter one.

5.1 Threats, risks, and/or vulnerabilities associated with the use of smartphones as working tools

There are numerous threats, risks, and/or vulnerabilities that could be associated with using the smartphone for work purposes if security is not prioritized by both the user and the one that assigns the device. Actions by users could open up opportunities or doors for malicious programs and users to exploit the organization. These risks increase when the organization makes it the sole responsibility of the user to configure his or her device for optimal security. As Botha et al. (2009) puts it, users are not always interested in optimal security but in the ease of use of their smartphones. Unlike on a computer where they are interested in secure passwords, users feel that smartphones do not require much of those security features due to their nature and how they are used.

Findings from this study indicate that just as Botha et al. (2009) and Landman (2010) indicated, there are some risks in the areas of expandable storage, physical threats, configuration and users, authentication, communication and applications.

As already highlighted by the literature review, every imaginable exploit that is associated with the use of computers can now be a threat for the smartphone as well. As the price of the

smartphone falls and its use becomes popular, attackers become interested in exploiting this new trend as they know that users might be unaware of the security limitations of these devices. It is not so much as to what trick they will use but rather of what the unsuspecting user does not know. Anything goes when it comes to cyber exploits today as long as the method selected will get the job done (Cisco, 2013, p. 51). Social engineering tricks are numerous. Each day something new that can be used to deceive at least one person is tried on someone. Features of the smartphone that make them very "smart" can put the phone in a lot of risks. The Samsung galaxy SIII and other Samsung devices created after the SIII smartphone have a feature called "S Beam" that allows it to share content with another Samsung devices that support S Beam, by gently bumping the backs of the phones together. Imagine that this feature is left opened. What kind of data could it be sharing with other devices? Respondents have services like the Bluetooth opened. They do not care enough to put any PIN on the phone itself and in cases where the PIN is used, they have not been changed from the default PIN of the manufacturer, are using PIN's that are easy to break or are displaying the characters of the PIN while they enter it to unlock the device. Respondents use the swipe security feature to secure their phones but instead of making the swipe pattern invisible so that shoulder surfers cannot see what pattern is used, they have the pattern displayed making it easy for any observer to try it out when they get access to the phone.

Respondents trust that their app store is secure enough to provide them with reputable applications. They seem to think that securing the smartphone is the sole responsibility of the providers of the device. That once the device is handed down to them, any security feature needed should have been implemented on them. The truth is that employees have different types of smart phones and though they may be from the same providers, they may have different configurations depending on which one the employee has. This makes it difficult for the information technology personnel to configure all these devices for optimum security as in each instance they may have to learn how the device works and what features makes them secure or insecure. The same can be said for other portable devices as well.

Respondents' knowledge of smartphone usage policies was not encouraging. It is either they knew it partially or didn't know it at all. They had been assigned company smartphones but nothing of policy was made available to them. If policies are made but are not disseminated, are not in the language that people bound by them can understand. If employees do not know what is acceptable and what is not, how can optimal information security be achieved?

Whether the phone was company assigned or not respondents found themselves using them for one or two personal activities such as checking their personal mails, making personal calls, downloading apps unto the phone and even playing games on the phone.

The interviews made use of five themes. These themes are Work and Mobility, General Questions about the Smartphones, Smartphones Security, Applications and Policy Related Questions. Below is a presentation of the findings from the interviews that sheds light on some of the threats, risks, and/or vulnerabilities associated with the use of smartphones as working tools.

5.1.1 Work and Mobility

As already highlighted in section 3.1.1, mobile workers use ICT to access remote information from their home base, workplace, in transit, and at other destinations (Kleinrock, 2001; Jacobs, 2004). It must be noted that mobile workers are not just workers who work outside their offices but also any worker that can work anytime and from anywhere, and any worker who demonstrates a high level of mobility within the workplace (Chen and Nath, 2011). Interviewees in the researcher's sample can be classified as mobile workers since they possess a great level of mobility at work. Respondents admit that they have varying rates of mobility from being slightly mobile to highly mobile depending on what they work with at any point in time and where they are. Apart from going for conferences, workshops or attending publications 2 to 3 times a year, respondents, shared that sometimes there was the need for work via their smartphones and other mobile tools such as laptops, PDA's and the likes. Respondents were away from their offices for periods of at most one week each month. While on such journeys, they particularly read and replied to emails, made and received calls and checked calendar schedules using their smartphones. Respondents also said that the same happened while they were on break or on the move within the confines of their work place. Though they preferred to work on their laptops, they admitted that there were some circumstances that prevented them from using the laptop. This made them choose the smartphone as it was more convenient in such circumstances.

Respondents said that they worked from home whenever they visited their family outside Sweden. Others also shared that since some courses taught were distance learning courses, they were able to teach from anywhere both from home and their offices or from the classroom with students joining from all over the globe. All they needed was an internet

connection. Because respondents could teach from home or campus and researched for companies outside campus, they had more than one office. This made them travel back and forth from one office to the other depending on what they had to do.

Respondents who were into research were able to do their research work wherever they were once they had internet connection. Surprisingly where they did not have internet connection on their laptops, they used the internet connection on their smartphones to connect their laptops so they could have a bigger working space as they claimed that it was a bit uncomfortable to work on the screen of the smartphone when there was much to do.

Findings from the interviews suggest that mobility is high within the younger generation. The same way, technology usage is also higher with the younger generation. Most workers prefer to transfer work unto their laptops while only making and receiving calls, checking and replying to emails and checking calendar schedules on their smartphone amidst using the smartphone for personal tasks such as playing a game, listening to music or reading the news. Reasons for this behaviour are one or all of the under listed:

- It is hard to use the small phone interface, or
- That there is more security on their computers than there is on their phone or
- That the cost of using the smartphone is higher in terms of charges than it is on computers.

5.1.2 The Smartphones

All respondents were in possession of a smartphone. The organization had assigned one to each person for work related purposes. In addition to the work assigned smartphone, respondents also had a personal smartphone. While respondents did not want to mix work related duties with personal duties when it came to the use of their smartphones, they did not mind at all. After all, they said, we have nothing more than making and receiving calls and checking emails. What's worse that could happen if we cross used our smartphones for work and personal duties. They affirmed this by indicating that they did not see anything important on their smartphones and so didn't think that using it this way could harm their organization.

When asked what activities they used their smartphone for it was interesting to note that all respondents used their smartphones for keeping a contact list, receiving and responding to

organizational specific emails, making and receiving calls and managing their schedules via the calendar on the smartphone. They sometimes extended the calling feature to the Skype application since it enabled them to make cheap calls from the internet. One admission was that when respondents were in meetings and needed to check their schedules, they preferred to do it on their smartphones because it was portable enough and didn't disrupt their meeting as doing same on a bigger device like a laptop may do.

When asked their thoughts about using the smartphones as working tools respondents responded in the affirmative. They said that in as much as they were good and must be encouraged they reduced their privacy too. Respondents said that though they felt they were old fashioned and rarely used all the features of their smartphones especially for work, they felt the smartphone was nice and handy and gave them very flexible opportunities. They went on to say that the smartphone was an excellent complement to the computer due to their portability and ease in carrying around. They also said that the smartphone should be encouraged because of the reduction in cost and an improvement in its processing ability. The smartphone they said gives us easy access to the things that we need access to like emails and contacts without having to dig into our bags and bring out our laptops. We do not have to go far and we do not have to travel to get it. When we are in the coffee room or in a restaurant during break, it is convenient to have our smartphone with us both for checking mails and picking calls or even checking our next schedule. The smartphone has become a reliable personal assistant to us. We can't always use the laptop in every place. Sometimes when we don't have internet on our laptop our smartphones help us to connect to its internet so we can continue to work. We value the ability to use our smartphone to connect to the computer in such instances. When we are far away from an electrical socket and our laptops have lost their power we can conveniently use our smartphone until we can find a place to charge the laptop.

On the other hand respondents said that they could be considered as both good and bad. You are always available in both good and bad instances. Respondents in order not to be disturbed admitted that they had configured their smartphones in order not to notify them whenever they had a new mail as this could disrupt them especially when they were in the middle of important meetings and could increase their stress levels. They preferred to check the mails themselves when they had time.

In spite of all the encouraging statements made about the smartphones, respondents felt that the smartphone was not very comfortable for voluminous work. For this reason where they had to do a lot of typing, they preferred to work on a bigger device such as on a laptop.

Respondents did not seem to think about the risks of using the smartphones as working tools beyond its cost implications. All respondents were particularly interested in the cost implications as this had been told to them by a colleague or someone who had experienced huge costs of roaming mobile data charges. To them using roaming mobile data was more damaging than any other risk as they could not even fathom what other risks they could run into. One interesting point noted was that though respondents knew there could be security risks, because they had not experienced any since they started using the device, and had not seen anyone in their working environment that had experienced it, they felt it was far away from them and didn't think about it much.

Respondents though were aware that "smartphone dumpster divers" purchased old and used phones just to get access to old data on the phones like credit card information and other personal data stored or even the contact list on the phones. They were also aware that if the smartphone was used to store confidential or private information and it was stolen, if the data had not been encrypted, anyone or the finder could read the data on the phone. Respondents believed that since hacking the smartphone was a new area for hackers, if they were extra careful with what they downloaded, they were safe and would remain safe. They explained that they had separated their work use of the smartphone from the personal use of the smartphone because they did not want to get into any serious information security risks. They also added that it was the reason why they kept two different sets of smartphones. This they said helped them to avoid installing infected or malicious apps on the work related smartphone that could end up sniffing data and conversations to unknown locations without their consent.

One thing stands out, once data can be created, stored or transferred from a smartphone to another device, and there are information security attacks such as man in the middle attacks, phishing attacks and the likes, it is imperative to be aware of what data one creates, stores or transfers and what security is put in place to limit the threats to these information created, stored or transferred from the smartphone. Though using the smartphone provides a cost effective way of making and receiving calls, reading and replying to emails and managing

work related schedules, if it is not controlled by the user carefully and intentionally things could get out of hand and confidential data transferred via emails or phone conversations could get into the wrong hands.

5.1.3 Smartphones Security

To be able to regulate and improve security via smartphones it is the duty of the organization to assign a smartphone to an employee. Respondents in this study also agree to this. They do not want to have to be burdened with the security concerns in addition to their numerous responsibilities at the work place. They accept that certain usage patterns could put the organization in harm's way but that the needed security settings and configurations must be done for them by the organization on the smartphone that had been assigned to them as Furnell et al. (2006) spoke about. They believed that when a company assigned a smartphone, the necessary configurations would be done before they were handed to the user or to the employee. Respondents say that they feel that with company assigned smartphones; the IT department had presumably tested the device to make sure that it functioned properly and that it fit the end-user's requirements and had optimal security on them.

Respondents shared that depending on what services the organization provides, it could have some mechanism put in place to secure their data. If an organization had product data and customer information for example, they could protect this by encrypting data in motion so that hackers would not be able to make sense of the data even if they were able to make copies of the data in transition. They could also allow access to their data only on a secure channel such as a VPN. On the other hand, for a university such as the one under study, they need more than a policy that prevents them from using data abroad because of its cost implications. They need to create and circulate policies that incorporate the smart features of the smartphone as the old phone usage policy seem to neglect these aspects and are not known by all employees. Most importantly there should be some education and training on these usage policies so that employees cannot claim they did not understand what the policies meant. The employees must be educated on how to use their smartphones for maximum benefits. Having a smartphone usage policy will make employees aware of the potential risks of using smartphones for work purposes. It will also make them aware of what they can and cannot do with their company assigned smartphone.

It is not surprising to see employees use BYOD's in addition to the company assigned smartphones. Respondents in this study had an additional smartphone for their personal use. In order to keep a high standard of information security, applications that the organization doesn't support must be disabled in its environs. One intelligent feature can be that company assigned smartphones have access to every application and resource that they need while BYOD's do not have any access to company resources. Since an employee's company assigned device can fail them any day, there should also be some chip INS that allows workers to use another device such as their BYOD to work but with permission from the organization. This should not be left to the discretion of the employee else this feature might be abused.

Policies and technical implementations should not be so much as to prevent the employee from working in any way or make their work difficult. Where this is the case, it is a norm to find employees finding other means and ways of working that might endanger the organization even more than if they had made some allowances for some freedom as Allam (2009) suggests.

Respondents suggested that having a mechanism to secure the organization's data resources was important irrespective of the type of ownership of the device. This they suggested was because any device whether company assigned or BYOD could circumvent the organization's information security. Respondents had no idea of which services were running wild on their smartphones. Some of these services could cause hackers to get into the organizations network or have access to contact details and other information that is stored on the phone without the user's knowledge. A feature that allows a smartphone to share data with another smartphone when they come into close contact with each other if not put off could cause the smartphone to share data without the user's knowledge. The organization must make a conscious effort to block services that they don't support and make employees aware of the risks involved when services are made opened especially Bluetooth.

While respondents believed that they performed no action that could cause the organization's information security to be circumvented or cause data to get into the wrong hand when the phone was lost or stolen, all of them admitted to checking their mails, always being on WI-FI, synchronizing their calendar schedules and even checking attached files in their mails on the smartphone. Because the device has been used for the activities listed above, there could be

traces of data and more importantly confidential data on the device. Examples of such data are the contact list, emails and other files that are downloaded unto the phone. Users do not always enter a username and password while checking an email on the smartphone. They preferred that this was done every once in at least 2 weeks or a month if they were using a browser. Where they were not using a browser, no username and password was required after the first username and password had been entered. This meant that if the phone got lost, anyone who found it could access the previous user's emails and make copies of important data.

Respondent suggested that they did not open company related files on their smartphones except for emails, student assignments and calendar schedules. They were more conscious of how to connect to the organizations resources. They suggested that when it was necessary to work via a smartphone, they would do just that. Depending on the volume of work that had to be done and where they were, they either worked on the smartphone or connected the smartphone to their laptops and worked from there. Respondents said though that they preferred to work on the laptop as it gave them more working space and a more secured environment. It is interesting to note that these respondents' who were not so keen on security on the smartphone chose very secure channels in connecting to browsers even on their laptops. They would only connect to https websites as this had more security than an ordinary http site.

On the topic on using anti viruses on smartphones, respondents' did not know such existed and so did not have any. The apple brand smartphone users suggested once more that their apps were secure and so didn't need an antivirus. They did admit though that without an antivirus, they could never tell if their phone had been compromised yet they did not have any installed on their smartphone. Again they were aware that smartphones had a mechanism to wipe out data when they were stolen but had not configured this yet. It all bores down to the fact that they felt that there was nothing confidential on the phone.

5.1.4 Application Installation on Company Assigned Smartphones

With the issue of installing additional application on the smartphone, respondents said that they did not do this on the company assigned smartphone except it was needed to do their work. They said though that they installed applications such as news readers on the work assigned smartphone so they could be informed about what was going on around them.

Maybe the organization could also look for feeds that reported on current security risks surrounding the use of smartphones as well as highlights on recent happenings with the smartphone so that users could be updated on these information security risks. They went on to suggest that the farthest they had gone was to install music applications like spotify on their smartphones. The most important aspect to the respondents was that once, it did not go against organization policy; they didn't see why they should not install an application if they needed it. This is a cause for concern and a great source of worry. How many users took time to check the names of the application they were about to install? For example to install spotify for music, users must be careful as there could be variants of spotify with one that has a space after the "y" such as "spotif y". Users must scrutinize the names and logos to be sure that they were the original that they were installing. Respondents also believed that the smaller the application of choice, the dangerous it was to install them as their trustworthiness could not easily be ascertained. Smaller applications could easily be hacked. Malware companies could also easily spread the malware through such applications. Respondents seemed to think that once they had used an application on the computers and had done some reading on them, they did not see why the application could not be installed on their smartphone. To them it was not so much of a long standing trustworthiness but the issues of that they had used it and it was problem free for them. On users personal smartphones not much care was taken to check and scrutinize these applications as users felt there was nothing confidential on these phones.

Surprisingly these phones were used on the organization's WI-FI. What if it served as a weak link through which the hacker could get unto the organization's network? Respondents indicated that to them the issue of installing a rogue application was not so much of a concern to them because they always installed from the app store. They never installed from any other place. They claimed that the issue of a rogue application was more damaging to the phone brand manufacturer than to the user. That in order to keep up the good name that a phone brand had, the producers of these phones had enough measures to prevent these bad applications from popping up on the app store. This was particularly true among the respondents that used the IOS branded smartphones. This presupposes that the respondents trust the manufactures of the phones and with the number of years in good standing had totally shifted the responsibility of good application to them. On a large scale it is true that these apps are checked. But from recent reports from the android users, IOS users and some other phone OS brand names, it is apparent that this is not always the case. Rogue applications can find their way onto the app store. Sometimes an application that was malware

free the first time it was installed can become infected later especially where users have made the update option automatic and had no antivirus to check the update file for traces of malicious content and activity.

When asked if users were aware their phone had been compromised, respondents said they could never tell if their antivirus programs did not inform them or they did not experience a change in speed of the smartphone.

5.1.5 Information Security Policy on the Use of Smartphones

A policy spells out a set of organizational guidelines that describe acceptable and unacceptable behaviours of employees within the workplace. It was surprising to know that the respondents did not know what exactly the smartphone usage policy stated. While they were aware of a phone usage policy in place that disallowed making private calls on the work assigned smartphone and avoiding roaming mobile data usage, they had not seen any policy in writing and could not affirm if what they knew was as a result of hearsay or from the experiences of their predecessors. Respondents had just been informed by their superiors and colleagues not to use mobile data when they were outside the country where their office was situated. They seemed to know that there was a policy about the cost implications of using their smartphones wrongly in terms of phone bills but not much beyond that. It was interesting to note that the only policies that respondents were aware of were not security related but cost related. These policies were only focused on how to cut down the cost incurred on the use of the smartphone when employees travelled outside the country. The smart aspects of the smartphone that could cause security breaches were not captured in the policy.

Respondents additionally added that there was policy on putting a PIN code on the smartphone to prevent just anyone from accessing the content of the phone. Though they believed that the use of the PIN code was not a bother, they saw it as a nuisance and so had none. The reason for not using one was because there was nothing confidential on the smartphone. Indeed there may not be anything special that needs to be protected on the smartphones, but what about all the resources that the phone owner can automatically access without having to enter a password or any authentication for? How can the user guarantee that it will always be them that would have access to the smartphone and not another person? If this cannot be guaranteed, then there must be a PIN code to disable easy access once anyone

picks up the phone. These smartphones may just be used to check emails most of the times but are the content of these mails always for public viewing? Are not some of the content organization specific and considered information for their competitive advantage? Would the organization or the department for that matter want this to be in the open space? If any of these answers to a NO, then there is indeed the need to prevent unauthorised people from having access to the content of these phones.

An issue of concern that arose was that though the policy stated no roaming mobile data, employees sometimes found themselves outside the country needing to attend important meetings and so went on to use roaming mobile data. Again though respondents were aware that they were not to use their company assigned smartphones for personal phone calls, they could not help but use it because to them the cost was insignificant if they called within the country where they worked.

Information security policies in an organization are as important as any other policy in the organization. Basically policies state what can and cannot be done within an organization. Policies must be up to date, they must be distributed to the employees they are written for, they must be in a language that can be understood by these employees and the enforcer of these policies must make sure that employees understand and agree to them. It is not enough to write a policy and stash it under the carpet only to bring them out when there is a breach in conduct. As technology improves and organizations become more technology centred, these policies must be updated to meet the new need.

5.2 Controlling Threats, Risks and/or Vulnerabilities Associated With the Use of Smartphones as Working Tools

The first approach to minimizing the threats, risks, and/or vulnerabilities associated with the use of smartphones as working tools is through the use of information security related policies for employees who use the device. This is because policies make employees aware of the dos and don’ts regarding the use of the device. These policies must be extended to inform and educate users on smartphone data wiping mechanisms, antivirus installations, applications allowed and not allowed and the likes. Organizations must also supplement policies with controls that help to enforce the don’ts on the employees’ smartphone. If certain applications must not be used or are not allowed on the company assigned smartphone, then employees should not be able to install them on the phone at all.

Policies should not prevent employees from working. Where this is the case, employees might find ways of working in order to keep their jobs and eventually cause the organization's information security to be circumvented. Take for example a situation where an employee travelling needs to have a business meeting on Skype but cannot find internet to connect with his laptop. He has a smartphone that has internet connection on it. Policy says that no roaming while abroad. But this meeting is important to the survival of the organization he works for. No client or customer would like to work with a partner who is not always there for them. They would rather have a partner who will provide them with the services they need anytime they want that service. Policies implemented must be made in such a way that such circumstances can be catered for. Policies formulated must ensure that employees connect only through secure channels when outside the organization. For example where a user doesn't connect through a VPN channel or through SSL sites they must not be allowed to connect. This way data from employee's device from point A to B would be encrypted preventing a hacker's readable access.

An information security culture as is described by Ghonaimy, El-Hadidi and Aslan (2002) and Schlienger and Teufel (2003) must be cultivated in the organization as these mould the attitudes and behaviour of the employees. It is important to note that when an organization has a very bad information security culture, every new employer that joins the organization is automatically drawn into these same attitudes. The new employee may adopt that attitude or might even be worse.

Companies must educate their employees on how to use their smartphones and other portable devices safely and especially for optimal security. Only applications that are supported by the organization should be allowed on company assigned smartphones while BYOD smartphones must not be allowed to access company related files and programs that the organization does not support.

Security must be seen as a top down approach not a bottom-up approach. If senior management is security conscious, lower members of the organization cannot be any different. They cannot make excuses that they don't know because it would be the priority of management to make it known and to enforce it.

Data classification can be implemented. This will help place extremely confidential information out of reach of unauthorised employees and especially via unauthorised devices such as BYOD's. The network could also be segmented so that areas that are accessible to employees via their smartphones while on the run outside their offices will be limited to those that are for the public.

Encryption of data must be enforced whenever employees send data from their smartphones to other resources. Organizations must adhere to standards such as the ISO27000 so as not to abuse the confidence that clients and share holders have in them with regards to their data.

For the smartphone user, the under listed can be done to control the threats, risks and/or vulnerabilities associated with the use of the device:

- Protect the smartphone physically and disallow others from using it.
- Backup your personal data from time to time.
- Be careful when you Wi-Fi as not all Wi-Fi are secured.
- Browse wisely choosing only secured sites that support encryption especially when there is the need to exchange sensitive information.
- Clear your cache.
- Have a data wiping mechanism installed on the smartphone.
- Do a little bit of reading on the apps that you want to install and check the names well to make sure you are not installing a counterfeit app.
- Check all permissions assigned to any app you want to install before they are installed.
- Don't throw or give away your smartphone without wiping all the data you have on it.
- Encrypt data on the device as well as data on any removable memory that the phone uses.
- Update your smartphone's OS as soon as it is released.

CHAPTER SIX
DISCUSSIONS

Analyzing the data gathered and the literature review made has helped to identify the apparent threat and negative consequence of the use of smartphones by employees to information security in an organization under the influence of mobility. This chapter presents a summary of threats, risks and vulnerabilities with the use of the smartphone and finally presents a discussion which leads to answering research question R.Q.3 in sections 6.2 and 6.3.

6.1 Threats, Risks and/or Vulnerabilities Associated With the Use of the Smartphone

As has already been highlighted by the literature review and the findings from this study, there are numerous threats, risks, and/or vulnerabilities that could be associated with using the smartphone for work purposes if security is not prioritized by both the user and the one that assigns the device. Every imaginable exploit that is associated with the use of computers can now be a threat for the smartphone as well. As Cisco (2013, p. 51) puts it, it is not the type of trick used that matters but what the unsuspecting user does not know. Besides what can be used to gain information or can be used to compromise one user's information security is not the same for another user. Any method that can at least get unsuspecting users to break their confidentiality, integrity or availability is used today. Actions like installation of apps without properly scrutinizing the permissions or using the device without a PIN or disposing of the phone without wiping the data off it or using an extended memory chip without encrypting it could cause users of the smartphone to compromise their information security. Malware-free apps can later on become infected because similarly to the malware BadNews reported by Help Net Security(2013), these apps may contain code which only becomes active after passing Google's scrutiny later on through the application's post-launch updates.

Analysis from the interview suggests that just as Botha et al. (2009) affirmed, users are not always interested in optimal security but in the ease of use of their smartphones though these same users may employ optimum security on their computers through secure passwords and lock screen among others. In general smartphone users feel that smartphones do not require much of those security features due to their nature and how they are used. Users of the device seem to use it as though it was either a purely social artefact or a purely technical artefact. They do not seem to consider it as a socio-technical tool that can boost the socio aspects of their working lives as well as the technical aspects of their working lives if managed as a

socio-technical artefact (Akbari & Land, 2005; Walker et al., 2008; Trist, 1981). The smartphone as a working tool can help maximize productivity if it is used as a socio-technical tool with the right education and training, the right controls and the right smartphone usage policies put in place. Unfortunately, givers of the smartphone and users of the smartphone do not realise that when the interaction of the social such as the employees, policies, knowledge, skills, attitudes, values and the technical factors such as machines, techniques and technological devices come together, it creates conditions for the success or failure of a system. With this in mind if the system is taken apart or is merged but does not incorporate the various items well, there could be lots of problems including the loss of sensitive information through the use of the smartphone.

Findings from this study also indicate that just as Botha et al. (2009) and Landman (2010) indicated, there are some risks in the areas of expandable storage, physical threats, configuration and users, authentication, communication and applications. Smartphone users do not consciously seek to put off services that are not needed. There were instances where Bluetooth had been left opened without the user knowing. Smartphones were not properly secured to prevent other people from having access to them. The reason being that there was nothing much on the device to demand stringent physical security measures. How do we achieve competitive advantage and create conditions for the success of our organization if the device that can lead people into our mail box where confidential matters are discussed, is left unprotected? Users were not aware that expandable memory chips could support encryption or that antiviruses could be used on the device. This could be because as at the time of the interview, respondents could not say what exactly policy stated about the use of the smartphone. The good thing is that none of the interviewees was using an extended memory yet. If information security policies were updated and were disseminated in an understandable language, it is likely that users would know what to do and what not to do and would understand the benefits of leaving or putting off a service that is not in use. With time the users of the device would adopt an information security conscious approach to the use of the device, thereby handling both the social aspect and the technical aspect of the device and creating conditions for high productivity while minimizing the loss of information to unintended recipients.

Individual smartphones and smartphone users have varying smartphone usage patterns. This presents important implications for the management of smartphone security risks. A

smartphone purchased for an employee for the purposes of work may have sensitive data stored on it or may serve as a gateway through which anyone that has access to the device can have access to organization specific data. This data could be data gathered on clients, or data that have been accessed by the employee via all sorts of apps on their smartphone as well as authentication credentials stored on the smartphone. Usually authentication is not done each time the user opens the browser to check emails or to access some of these organizational resources via a browser. Users of the smartphone enter authentication details once in a while as they believe the smartphone is personal and is used by them alone. Users of the smartphone move about within the organization as well as outside the organization. While on holidays some employees carry the device along. Be it a personal smartphone or an organization owned smartphone, the device is used to access open Wi-Fi as the user travels around. Not all these hot spots can be trusted. Some of these open connections are owned by scrupulous people who are sniffing around for any confidential data they can lay their hands on. Access to any organization's data could be used to black mail the organization into giving them what they want or could be used against the organization to wane its trustworthiness to the public. If a malicious person gets access to client data, this could cause the organization to end up in suits that could cost the organization huge sums of money and eventually cause the organization to close down. A smartphone acquired purposely for work, may be used for personal social networking during weekends and for handling sensitive email on working days. The implications of using the smartphone for both work purposes and personal purposes imply a possible breach of the confidentiality, availability and integrity of the organizational data resources (Fitzgerald, 2009).

Smartphones often contain valuable information such as credit card data, bank account numbers, passwords, contact data, corporate emails and corporate documents which may have sensitive data contained in them. The smartphones may also have schedule information, email credentials and other credentials to sites browsed by the user of the device. They are often the user's primary depot of personal data because of the ease of carrying it everywhere, its availability and ubiquitous connectivity. Unfortunately users believe that there is not much on their smartphones and that their device cannot be a source of threat to the information security of their organization. They do however admit that they have a contact list, they read and reply to emails, have a schedule of meetings on the device and have some apps installed on the device.

When asked how these users can ascertain the app installed for its trustworthiness, the common answer given was that the phone manufacturer could be trusted and so any app installed through the app store could also be trusted. Users have shifted the responsibility of checking for the trust worthiness of an app to the phone manufacture, they believe that because these phone manufactures don't want their name to be dragged in the mud, they scrutinize the apps that are available on the app store to prevent any breach of security.

It is interesting to note that users were not aware that antivirus programmes could be used on the device let alone know which ones could best serve their needs. Users were not interested in optimal security because they saw it as a tedious task as they had to provide these every time they wanted to use the device. Due to the small nature of the device and the miniature version of keyboard on the device, they tried to minimize the security settings as much as possible. Where PIN's had to be used, users either ignored it, used the default PIN's or used a weak one. Again a swipe mechanism in place was visible to shoulder surfers and in some case, both the PIN and swiping functionality had been ignored completely.

With the increase in apps on the app store for almost anything under the sun, it is difficult to know which app has no malicious intent if there is no antivirus to help check for malicious intent or if the permissions requested for by the app is not checked properly. A malicious app installed on a smartphone could serve as a gateway through which data could be collected from the smartphone to another location where the bad guy wants the data collected. Connecting to open Wi-Fi which do not have encryption could mean that any data transfer on such networks are freely available to whoever cares to make copies of them. Due to the mobility of these workers and the need to respond to clients and employers irrespective of where employees are, they could easily be giving out confidential corporate data while browsing on such links. This may lead to a breach in confidentiality and subsequently to a breach in the integrity of the data being transferred as the sniffer could alter the data in transit.

Not all users of the smartphone are aware of all the functionality of the device they are using or the apps that they have chosen to install on their smartphones. By ubiquitously using a smartphone, the user may disclose data unintentionally. One such common data is location data. Though most apps have privacy settings for controlling how and when location data is transmitted, many users are unaware that the data is being transmitted, let alone know of the existence of the privacy setting to prevent this. Unintentional disclosure of location data may

help attackers to track and trace users and so allow, for example, stalking, robbery or the hijacking of trucks containing valuable goods (Enisa, 2010).

As the smartphone evolves and technology gets better, there is the tendency that users of the device will give them up for better ones with more applications. This makes the approach used to recycle the smartphone very important to users and to the organizations that give them Enisa (2010). As previously mentioned, smartphones contain large amounts of sensitive information which may be valuable to an attacker. This makes it an increasingly attractive target for smartphone dumpster divers. How an organization disposes of its used and unwanted smartphone previously used by an employee is very vital to the survival of the organization. When an employee's contract has been terminated, or when an employee leaves the organization, the smartphones given to them is taken away from them. These phones could be sold to generate money for the organization or could be given to another employee to be used. There is the need whatever the use of that phone would be when disposed, to clean the device of all data held on it. Preferably it must be reset to its original state and all data erased. This will prevent smartphone dumpster divers from having access to data previously stored on the device.

Enisa (2010) reports a case in which mobile phones bought second-hand on eBay had 26 of them being business smartphones. Of the 26 business smartphones sold, 4 contained information from which the owner could be identified while 7 contained enough data to identify the owner's employer. The research team managed to trace one smartphone to a senior sales director of a corporation, recovering call history, address book entries, diary, emails, etc.

6.2 The Challenge that Mobility puts on Information Security

Information Security gives an assurance that information risks and controls are in balance as Whitman and Mattord (2004) suggest. Employees depend on the use of ICT to perform almost all aspects of their job roles and so can be classified as mobile workers as Kleinrock (2001) and Jacobs (2004) suggest. The basic aim of information security is to provide confidentiality, integrity and availability. These can be optimally possible to achieve if all devices are confined to one place and within the control of the organization but in reality this is not the case. Employees are mobile in and out of the office. These types of workers are free from the spatial and/or temporal constraints of the traditional office as Balasubramanian et al. (2002)

put it. With the help of mobile computing technologies, the gap between these workers and the information they need for work is seamless (Chen & Nath, 2003). Whether it is leaving the house to work, attending to business partners, clients and colleagues in the office or providing services to clients in their office environment, employees are in one way or the other left with no option but to extend work via a portable device such as the smartphone. Different environments support different levels of security. One can only be the best in their environment and hope that they can control to some extent how people connect to them and what they have access to.

Smartphones, due to their high mobility challenges information security in several ways. The fact that these devices can be somewhere that the organization cannot have complete control over makes the issue of security a complicated and daunting task. The discussion that follows provides a summary of how mobility challenges the information security needs of an organization through the lens of confidentiality, integrity and availability.

To enforce confidentiality is to restrict information access to only those who must have access to the information. With the emergence of smartphones and their mobile nature, this cannot always be achieved. As employees travel about both within and outside their organizations, they are forced to use open Wi-Fi connections that cannot be secured by their organization. These networks are composed of good users as well as bad users whose job is only to sniff data transferred. Even when the smartphone user uses their own mobile data, the transfer of data from their device is not always encrypted. Some apps through which they transmit data send the data in an unsecured channel, causing information spillage into the wrong hands.

If an employee travels and they want access to their organization's information resources, they may use open Wi-Fi or the mobile data from their smartphone. In most cases to avoid incurring huge roaming mobile data charges, they make use of open Wi-Fi connections. Open Wi-Fi connections are not implemented for optimal security. Its open nature means that it cannot be secured because if it is secured, then it cannot be open for everyone to be able to use them. Such networks obviously are not controlled by the organization of the employer. These Wi-Fi connections could be infected causing the user to infect his organizations resources in the process of connecting through that channel to the works resources. They could also have men-in-the-middle who sniff around to capture any data sent unencrypted via such connections. An open and unsecured connection could lead hackers to enter into the

organizations data resources and depending on what kind of data resources the organization generates, the company could lose, especially if the organization deals with product data or customer data.

Smartphones that connect to an organization's resources though may have been authenticated and authorized to access organizational data, could be doing so through apps that store sensitive details on the phone without the user's knowledge. It may also be possible that cookies and other malware present on the phone logs whatever the user does and sends them to an unauthorized person or location somewhere.

Smartphone users cross-over from one usage scenario to another. This could cause a lot of information security risks. For example, a work assigned smartphone with sensitive data could be taken outside the country of residence where the organization is situated on holiday by an employee. This could easily cause cross-border data flow. Another scenario is where a work assigned smartphone is used for personal social networking during weekends and for handling sensitive email on working days.

As the users move around, the apps that they have installed on their smartphones have privacy settings for controlling how and when location data is transmitted, but not all users are aware or even recall that they have their personal data being transmitted in the background while they are on the go, let alone know of the existence of the privacy setting to prevent this. Such location data may often be used in social networks, in messages or uploaded photo metadata, in augmented reality apps, micro-blogging posts, etc. An application like Viber, which is used for making and receiving calls, allows the user to display their current address by a click in the same the textbox where messages are typed. Not all users are aware that by clicking on the small arrow in the textbox in Viber, they are sending as part of the message typed their address. These same users because they do not know how they turn on the location address in Viber may also not know that by clicking on the same area they put of the location address. Unintentional disclosure of location data may help attackers to track and trace users and so allow, for example, stalking, robbery or the hijacking of valuable goods and other items as is reported by Enisa (2010). Unlike during downloads of files where the user gives his consent, the same cannot be said for location data. It is not feasible for the user to have to consent every time a new location is disclosed.

For confidentiality to be properly enforced, measures must be implemented across all mediums of information storage, communication and processing for true restriction of access to be enforced. This cannot be done when the smartphone is moved around and made to communicate with all sorts of networks and applications that are not controlled by the user's organization.

Additionally because the smartphone can be taken everywhere the user wants to go, the probability that it can get lost is high. With the user's attitude not optimally focused toward information security, it becomes difficult for confidentiality to be achieved even when the best technology has been put in place to enforce this. Once the phone is lost or stolen if the phone uses an unencrypted memory card, all the data on it can be read. Again if default passwords are used, they can easily be broken and everything on the phone will be accessible to the finder of the phone. To carry a smartphone around with all the data it is used to access is like carrying the whole or a part of an organization's data resources around thinking that it is safe in the hands of the holder because they would never let go for someone else to have access to them.

Failure to enforce confidentiality means an indirect failure to achieve integrity. When confidentiality has been broken, it does not take much to break the integrity of data. Integrity enforces accuracy, authenticity and trustworthiness of information and information resources. In most cases once data unintended for the bad guy to see, has been given to them consciously or unconsciously, it does not take them too much effort to change or temper with the data. A man-in-the middle can easily change the content of data that is been transferred in plain text if he can read what is being sent or if he can break weak encryption set on data in transit. This is the reason why when a choice of encryption is opted for, the best and most difficult to break must be selected. What cannot be broken today may be broken in a few seconds tomorrow. If confidentiality cannot be assured while using the smartphone, then undesired modification of information cannot also be assured. If smartphones were confined to a solitary area where IT Officers had control over, this could be minimized to the barest minimum. Since this is not the case, enforcing the integrity of data in the midst of mobility becomes a challenge.

Integrity is important as organizational information must be maintained in formats best suited to the business context that they support. Any malicious or accidental modifications can and

may result in information that no longer provide competitive advantage to the organization and employees that use it.

The Integrity of data can be protected only when the confidentiality of the data can be guaranteed. Since smartphones can communicate in unsecured channels such as open Wi-Fi by other people other than the organization for whom the employee works, ensuring integrity, through confidentiality becomes complicated (Allam, 2010). Ensuring the integrity of the information received and sent on untrustworthy channels and networks is important in order to achieve adequate information security.

To achieve availability which is the third basic component of information security is to be able to access information and information resources as and when needed. To be able to extend information access to employees outside the organization means to make use of untrustworthy networks outside the information security management of that organization. To enjoy competitive advantage an employee must be able to make use of the data generated by an organization no matter where they are and be able to keep this information from getting into the open especially to organizations that produce similar products or services. In a bid to provide mitigation strategies for untrustworthy communication channels via smartphones employees could be restricted access to data they need for work when they are outside the confines of the organization they work for. This could reduce productivity and slow down decision making processes. On the other hand if these mitigation strategies are not put in place data could easily get into the wrong hands thereby causing the organization to lose its competitive edge over similar organizations. As a result of the nature of smartphones and their high mobility, where to put availability has become a challenge. If it is taken out, an organization might lose. At the same time, if it is not properly implemented, the organization loses. Knowing where to draw the line is a great headache for Information Security personnel and management.

All components of information security must be met for optimal information security. Leaving one out of the three could cause even those that have been implemented to be circumvented. There cannot be a weak link in this kind of chain else the whole chain is weak.

6.3 Addressing Mobility and Information Security Problems Using the Socio-Technical Theory.

The socio-technical theory as already discussed further up section 3.2 in the theoretical framework suggests that it recognizes a system as having a technical component as well as a social component (Trist, 1981). Information security on the other hand though recently tries to take care of the human factor as Kruger and Kearny (2008) and Dhillon and Backhouse (2000) suggest, sometimes gives little room for the social aspect of the system to be fully addressed. Kisling (2006) report that for any technical system to be effective, the social system must also be effective.

If information security can be successfully implemented, the organization that chooses it must take into consideration the human factor. After all, the human is the weakest link. No matter what implementations there are to secure organizational data, if the employee does not adhere to them, it would serve no purpose. The technical information security solutions that organizations provide are used by humans and as such the human aspect must also be taken into consideration. The olden days saw IT Personnel securing all computers and having complete control over these devices. Smartphones though may have been purchased by an organization to be used by an employee is not managed the same way as a computer that belongs to an organization. To some extent the user of the smartphone has a lot of say as to how it should be configured. Unfortunately not all users possess the technical knowhow of how to securely configure their smartphones to support the organizations information security needs. As Furnell et al. (2006) report, some users will actively seek to overcome secure configurations, whereas the most likely scenario is that security configurations will be unused or configured incorrectly thereby exposing the organization to risks.

Organizations must be willing to improve the employee's knowledge, skills, attitudes, values and needs they bring to the work environment through education and training towards a secure environment rather than just implement some technical boundaries that can easily be circumvented by these employees (Akbari & Land, 2005; Walker et al., 2008). After all, that is the purpose of the social aspect of the socio-technical system; to incorporate the employee's knowledge, skills, attitudes, values and needs into the work environment to yield the maximum benefits to both the organization and the employee. Since employees are highly mobile and sometimes use mobile devices to work while away from their offices, it is important that part of the knowledge, skills, attitudes, education and training that the

employer inculcates into the employee include secure ways of communication outside the confines of the organization.

It is interesting to note that though socio-technical theory emphasises the use of policies in organizations to guide employees in what to do and what not to do, some organizations do not have updated policies. Some organizations still operate under the old policies that were drafted when the organizations came into being but keep putting up controls to help curb the information security menace woefully. Organizations are not static entities. They grow and they change. As and when these changes take place, the policies in place must reflect the changes. In situations where policies are available, they have not been distributed to the targeted audience. Policies for mobile phone may not necessarily be for smartphones. Mobile phone usage policies may only be interested in avoiding costs of mobile data abroad. Meanwhile the implications of misusing a smartphone for work could cost more than the cost of mobile data abroad. If client data gets into the wrong hands, it could cause an organization to suffer huge fines in law suits and eventually wane the reputation of the organization and even lead to the collapse of that organization.

Developing an information security centred organizational culture is important in shaping the attitudes of employees and moulding their work manners. Culture is a way of life. If the right culture is cultivated in the working environment most of the challenges of what to do, what not to do and how it must be done will be solved or reduced to the barest minimum.

In summary, for an organization to be able to benefit from the use of the socio-technical theory they must provides a solution based on all the following:

- Policy and Procedure
- Education and Training
- Technology and Controls

Organizations are dynamic and so one solution cannot fit all organizations. Whatever solution is developed based on the above mentioned depends on what kind of organization it is and what kind of data the organization produces as well as the knowledge base and skill of the employees.

CHAPTER SEVEN

CONCLUSION

This study highlighted the perceived or experienced threat and negative consequence of the use of smartphones by employees to information security in an organization. The study also analyzed the effects of the use of smartphones by mobile workers on the information security of an organization and identified the most significant threat and risk areas of the use of smartphones within an organization. Some counter measures that could facilitate a relatively threat free working environment with the use of the smartphones were suggested. Finally, the challenges of mobility on the information security needs of an organization were discussed and the socio-technical theory was used to address the problems that smartphones through mobility pose in information security.

Choosing which device to use for work should not be limited to a smartphone, a laptop or any form of portable device but to the device that comes in handy and convenient as and when needed. It might be easier to check emails on a smartphone while in the bus than it is to check same on a laptop in the same location. It may not be convenient to work on large volumes of data in an office or in a room from a smartphone. Smartphones cannot be completely eliminated from the lives of employees. They extend work beyond the office and help to stay connected while on the run. With the use of appropriate policies and the right technological strategies in place, the risks could be brought to the barest minimum while its benefits are optimized.

As Information Technology develops and smartphones improve, the users' usage patterns change. Today's research might not explain the phenomenon of tomorrow's situation very well, so this research can only explain the phenomenon in this specific case and for this particular time and place. When future researchers use these research results, they need be aware of all these factors to maintain the objectivity of their studies.
The concluding remarks and findings of this study are summarized below:

Threat: Smartphone threats are diverse and are a reality instead of a fairytale. As the price of the smartphone reduces and their functionality improves, the number of its users increases. This makes it a target for hackers and malware as they can exploit the device to gain personal and organizational data.

Perception: The perception of users on the risks of using a smartphone for work is not as high as can be. Users still think that if only the phone is used for making and receiving calls, reading and replying to emails and checking calendar schedules, then there is nothing much to protect. In reality this is not the case. Smartphones have a lot more going on them than just the aforementioned. Users must be educated on the reality of the matter and be made aware of the current risks there are so as to increase their consciousness on this matter.

Countermeasures: There are numerous counter measures that can be employed when embarking on smartphone security. The choice of a counter measure depends on factors such as what kind of data the organization produces as well as what kind of usage patterns employees have. There is no one size fit all counter measure that can be implemented. Organizations must realize this and embark on the best solutions that are suitable for their organization. To get the best counter measures in place, organizations should make their own risk assessments and weigh the risks against the potential benefits in their own specific cases.

Workforce Mobility: Though employees may not always admit it, workers these days are very mobile. Being mobile at work does not only mean travelling outside your place of work to another office location or country. Mobile workers consist of those workers who move about a lot even in their offices. To be able to stay on top and maintain competitive advantage demands that employees respond to their clients and employers anywhere, anytime. Smartphones make this possible when computers and other devices cannot be used.

7.1 Future Work

One qualitative study cannot explain every possible scenario of what can happen when smartphones are used as working tools especially when different organizations have different needs and produce different kinds of data. Most importantly, the mobility of employees varies. The potential future research in continuation of this study includes:

- Extension to mobile workers who are heavily dependent on the use of smartphones in their daily activities in organizations such as consultancy firms, workers in the mining industry and workers in the oil industry who commute a lot for work purposes, etc. Various groups from these organizations could be researched and the outcomes compared. This will help shed more light on the reality of the integration of the smartphone as working tools.

- A practical experimental setup to investigate the security of the different smartphone operating systems as we have today and how susceptible they are to mobility and information security.

REFERENCES

Ahmed, M. H., Penney, J., Ikki, S., Salami, A., Bath, T. L., Allah, M. A., & Mansour, S. (2009). *Threats to Mobile Phone Users' Privacy*. Memorial University of Newfoundland, St John's, NL, Canada.

Akbari, H., & Land, F. (2005). Theories Used in IS Research: Socio-Technical Theory. Retrieved February 18, 2013, from http://www.istheory.yorku.ca/sociotechnicaltheory.htm

Allam, S. A. (2009*). A model to measure the maturity of Smartphones security at software consultancies'*, Faculty of Management and Commerce of the University of Fort Hare

Allam, S. (2011). An Adaptation of the Awareness Boundary Model towards Smartphones Security. *Information Security South Africa (ISSA)*

Arthur, C. (2011). More Than 50 Android Apps Found Infected With Rootkit Malware. Retrieved March 15, 2013, from http://m.guardian.co.uk/technology/blog/2011/mar/02/android-market-apps-malware?cat=technology&type=article#

Balasubramanian, S., Peterson, R., & Jarvenpaa, S.L. (2002). Exploring the Implications of M-Commerce for Markets and Marketing. *Journal of the Academy of Marketing Science*, 30 (4), 348–361.

Ballano, M. (2011). Android Threats Getting Steamy | Symantec Connect Community. Retrieved March 17, 2013, from http://www.symantec.com/connect/blogs/android-threats-getting-steamy#

Banks, L. (2010). Mobile Devices Pose Security Dilemma for CIOs. Retrieved February 10, 2013, from http://www.cio.com.au/article/346474/mobile_devices_pose_security_dilemma_cios/

Basole, R.C. (2008). Enterprise Mobility: Researching a New Paradigm. *Information Knowledge Systems Management*, 7, 1–7.

Berelson, B. (1952). Content Analysis in Communication Research. Glencoe, Ill: Free Press.

Berg, B.L. (2001). Qualitative Research Methods for the Social Sciences.Boston: Allyn and Bacon.

Beurer-Zuellig, B., & Meckel, M. (2008). Smartphones Enabling Mobile Collaboration. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual* (p. 49). Presented at the Hawaii International Conference on System Sciences, Proceedings of the 41st Annual. doi:10.1109/HICSS.2008.399

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective PART II: The Application of Socio-Technical Theory. *MIS Quarterly* 1(4), 11–28.

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From Desktop to Mobile: Examining the Security Experience. *Computers & Security*, *28*(3-4), 130–137.
Boyce, C., & Neale, P. (2006).Conducting In-Depth Interviews: A Guide for Designing and Conducting In-Depth Interviews for Evaluation Input. *Pathfinder International Tool Series*

Bradley, J. (1993). Methodological issues and practices in qualitative research. *Library Quarterly*, 63(4), 431-449.

Büscher, M., & Urry J. (2009). Mobile Methods and the Empirical. *European Journal of Social Theory* 12(1), 99–116.

Chen, L., & Nath, R. (2003). A Framework for Mobile Business Applications. *International Journal of Mobile Communications*, 2(4), 368–381.

Chen, L., & Nath, R. (2006). An Empirical Examination of the Impact of Wireless Local Area Networks on Organisational Users. *Journal of Electronic Commerce in Organisations*, 4 (2), 62–81.

Chen, L., & Corritore, C. (2008). A Theoretical Model of Nomadic Culture: Assumptions, Values, Artefacts and the Impact on Employee Job Satisfaction. *Communications of the AIS*, 22, 235–260.

Chen, L., & Nath, R. (2008). A Socio-Technical Perspective of Mobile Work. *Information Knowledge Systems Management*, 7, 41–60.

Chen, L., & Nath, R. (2011). Impediments to mobile work: an empirical study. *International Journal Of Mobile Communications*, *9*(5), 522-540.

Chia, P., Maynard, S., and Ruighaver, A. (2003): Understanding Organisational Security Culture, In Hunter, M. G. and Dhanda, K. K. (Eds.) Information Systems: The Challenges of Theory and Practice, Information Institute, Las Vegas, USA, pp.: 335 – 365.

Cisco (2013). Cisco Annual Security Report. Retrieved February 10, 2013, from http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html

Clarke, N., and Furnell, S. (2007). Advanced User Authentication for Mobile Devices. *Computers and Security*, 26 (2), 109-119.

Conlin, M. (2006). Smashing the Clock. *Businessweek*, 60–68.

Connolly, P. J. (2000). Security Starts from Within. *Info World*, 22(28)

Corbin, J., & Strauss, A. (1990). Grounded Theory Research: Procedures, Canons, and Evaluative Criteria. *Qualitative Sociology*, 13(1), 3-21.

Couture, E. (2010). *Mobile Security: Current Threats and Emerging Protective Measures*. SANS Institute InfoSec Reading Room. Retrieved November 7, 2012, from http://www.sans.org/reading_room/whitepapers/incident/wireless-mobile-security_33548
Cresswell, T. (2006). *On the Move: Mobility in the Modern West*. London: Routledge.

Cyber Future Will Bring Mixed Blessings. (1996). *USA Today Magazine, 124*(2613), 4.
Ruggiero, P., & Foote, J. (2011). *Cyber Threats to Mobile Phones*. Carnegie Mellon University. US-CERT. Retrieved November 05, 2012, from http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf

Daniel, D. (2008). Human Error Tops the List of Security Threats. Retrieved December 17, 2012, from http://www.cio.com/article/179802/Human_Error_Tops_the_List_of_Security_Threats

DeSanctis, G., & Poole, M.S. (1994). Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory. *Organization Science*, 5 (2), 121-147.

De Wever, B., Schellens, T., Valcke, M., & Van Keer, H. (2006). Content Analysis Schemes to Analyze Transcripts of Online Asynchronous Discussion Groups: A Review. *Computer & Education*, 46, 6-28.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. Association for Computing Machinery. Communications of the ACM, 43(7), 125-128.

Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers and Security*, 20(2), 165-172.

Drew, M. (2006). Bringing Enterprise Mobility to Industry. *Manufacturers' Monthly*, December, pg. 28.

Dunn, J. E. (2011). Mobile malware exaggerated by "charlatan" vendors, says Google engineer - PC Advisor. Retrieved February 15, 2013, from http://www.pcadvisor.co.uk/news/network-Wi-Fi/3320818/mobile-malware-exaggerated-by-charlatan-vendors-says-google-engineer/

Dunning, J. P. (2010). Taming the Blue Beast: A Survey of Bluetooth Based Threats. *IEEE Security & Privacy*, *8*(2), 20-27.

Eason, K. (2001). Changing Perspectives on the Organizational Consequences of Information Technology. *Behavior & Information Technology, 20*(5), 323-328.

Elgan, M. (2007). It's Time We Stopped Talking About Smartphones. Retrieved December 31, 2012, from http://www.techworld.com/mobility/features/index.cfm?featureid=3204

Enisa (2010). Smartphones: Information Security Risks, Opportunities and Recommendations for Users. Retrieved April 25, 2013, from https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users

Ernest-Jones, T. (2006). Pinning Down a Security Policy for Mobile Data. *Network Security*, 6, 8–12.

Ernst & Young (2011). Into the Cloud, Out of the Fog - Ernst & Young's 2011 Global Information Security Survey. Retrieved February 21, 2013, from http://www.ey.com/Publication/vwLUAssets/Into_the_cloud_out_of_the_fog-2011_GISS/$FILE/Into_the_cloud_out_of_the_fog-2011%20GISS.pdf

Fitzgerald, J. (2009). Managing Mobile Devices. *Computer Fraud & Security*, 2009(4), 18-19.

Fratto, M. (2009). 2009 Strategic Security Survey. Retrieved February 21, 2013 from http://i.cmpnet.com/custom/strategicsecurity/assets/InformationWeek_Analytics_2009_Strategic_Security_Survey.pdf

Furnell, S., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers and Security*, *25*(1), 27–35.

Furnell, S., and Thomson, K.-L. (2009). Recognising the Varying User Acceptance of IT Security. *Computer Fraud and Security* (2), 5-10.

Gartner (2009). Gartner Glossary. Retrieved December 31, 2012, from http://www.gartner.com/6_help/glossary/GlossaryS.jsp

Carabott E., (2009). Taking Security Seriously. Retrieved February 21, 2013 from http://www.gfi.com/blog/taking-security-seriously/

Ghonaimy, M. A., El-Hadidi, M. T., & Aslan, H. K. (2002). Security in the Information Society:Visions and Perspectives. *Kluwer Academic Publishers*

Hannam, K., Sheller, M., & Urry, J. (2006). Editorial: Mobilities, Immobilities and Moorings. *Mobilities*, *1*(1), 1–22.

Heikkila, F. M. (2007). Encryption: Security Considerations for Portable Media Devices. *Security & Privacy, IEEE*, *5*(4), 22–27.

Help Net Security (2013). Researchers Discover more BadNews on Google Play. Retrieved April 29, 2013, from http://www.net-security.org/malware_news.php?id=2475#

Hildenbrand, J. (2012). Android 4.2 brings new security features to scan sideloaded apps | Android Central. Retrieved February 15, 2013, from http://www.androidcentral.com/android-42-brings-new-security-features-scan-sideloaded-apps

Hoang, A.T., Nickerson, R.C., Beckman, P. and Eng, J. (2008). Telecommuting and Corporate Culture: Implications for the Mobile Enterprise. *Information Knowledge Systems Management*, 7 (1–2), 77–97.

Holsti, O.R. (1969). Content Analysis for the Social Sciences and Humanities. Reading, MA: Addison-Wesley.

Hsieh, H. F., & Shannon, S.E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, 15(9), 1277-1288.

Hughes, M., and Stanton, R. (2006). Winning Security Policy Acceptance. *Computer Fraud and Security*, 2006 (5), 17-19.

Jacobs, G. (2004). Diagnosing the Distance: Managing Communication with Dispersed Technical Workforces. *Corporate Communications*, 9(2), 118–127.

Johnson, J. (2009). Memory Cards for Your PDA: Expand Your PDA's Storage Potential. Retrieved December 31, 2012, from http://palmtops.about.com/od/accessoriesperipherials/ss/flashcards.htm

Juniper Networks (2011). Mobile Device Security, Emerging Threats And Essential Strategies - Key Capabilities For Safeguarding Mobile Devices And Corporate Assets. White paper, Juniper Networks, Inc.

Jürjens, J., Schrek, J., & Bartmann, P. (2008). Model-based Security Analysis for Mobile Communications. *ACM International Conference on Software Engineering*, 683-692

Kisling, E. L. (2006). An implementation of information technological change: A socio-technical systems methodology perspective at the black chemical company. Indiana University. ProQuest Dissertations and Theses, 347-347

Kim, B., & Han, I. (2009). What Drives the Adoption of Mobile Data Services? An Approach from a Value Perspective. *Journal of Information Technology*, 24 (1), 35–45.

Kleinrock, L. (2001). Breaking Loose. *Communications of the ACM*, 44(9), 41–45.

Kothari, C, (2009). Research Methodology: Methods and Techniques. *New Age International*

Krippendorff, K. (1980). Content Analysis: An Introduction to Its Methodology. Newbury Park, CA: Sage.

Kritzinger, E., and Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers and Security* , 27 (5-6), 224-231.

Kruger, H. A., and Kearny, W. D. (2008). Consensus Ranking – An ICT Security Awareness Case Study. *Computers and Security*, 27 (7-8), 254-159.

Kvale, S. (1996). Interviews: An Introduction to Qualitative Research Interviewing. Thousand Oaks, CA: Sage Publications, Inc.

Landman, M. (2010). Managing Smartphones Security Risks. *Information Security Curriculum Development Conference*,145-155

Levine, J. H. (2007). Introduction to Data Analysis: The Rules of Evidence. Retrieved February 09, 2012, from http://www.dartmouth.edu/~jlevine/stuff/intro%20copy/introfrset.html

Liginlal, D., Sim, I., and Khansa, L. (2009). How Significant Is Human Error as a Cause of Privacy Breaches? An Empirical Study and a Framework for Error Management. *Computers and Security*, 28 (3-4), 215-228.

Lincoln, Y.S., & Guba, E.G. (1985). Naturalistic Inquiry . Beverly Hills, CA: Sage Publications.

Lopez-Nicolas, C., Molina-Castillo, F.J., & Bouwman, H. (2008). An Assessment of Advanced Mobile Services Acceptance: Contributions from TAM and Diffusion Theory Models. *Information & Management*, 45 (6), 359–364.

Lyons, G., & Urry, J. (2005). Travel time use in the information age. *Transportation Research Part A: Policy and Practice*, *39*(2-3), 257-276.

Maconachy, V. W., Schou, C. D., Ragsdale, D., & Welch, D. (2001). A Model for Information Assurance: An Integrated Approach. *IEEE Workshop on Information Assurance and Security*, 306–310.

Mahoney, C. (2009). Talk Generation Y's Language. *HR Magazine* , 25

Manz, C. C. & Stewart, G. L. (1997). Attaining flexible stability by integrating total quality management and socio-technical systems theory. *Organizational Science, 8*(1), 59-70.

Martins, A., and Eloff, J. (2001). Information Security Culture. Retrieved December 12, 2012, from http://etd.rau.ac.za/theses/available/etd-04292004-10222/restricted/SEC2002FinalVersion.pdf -12th December,2012

Mayring, P. (2000). Qualitative Content Analysis. Forum: Qualitative Social Research, 1(2). Retrieved June 17, 2013, from http://217.160.35.246/fqs-texte/2-00/2-00mayring-e.pdf.

McDonough, C. (2003). Identifying the Risk Involved In Allowing Wireless Portable Devices Into Your Company. *InfoSec Reading Room*. SANS Institute

McDowell, M. (2008). Business Mobility: A Changing Ecosystem. *Information Knowledge Systems Management*, 7, 25–37.

McIntosh, J.C., & Baron, J.P. (2005). Mobile Commerce's Impact on Today's Workforce. *International Journal of Mobile Communications,* 3 (2), 99–113.

Michael, H. (2012). Android malware perspective: only 0.5% comes from the Play Store. Retrieved February 15, 2013, from http://www.phonearena.com/news/Android-malware-perspective-only-0.5-comes-from-the-Play-Store_id36696

Moody, D., & Walsh, P. (1999). *Measuring the Value of Information: An Asset Valuation Approach.* University of Melbourne, Department of Information Systems, Melbourne

Musaji, Y. (2006). A Holistic Definition of IT Security—Part 2. *Infromation Controls Journal (ISACA)*

Olzak, T. (2006). Strengthen Security with an Effective Security Awareness Program. Retrieved December 17, 2012, from http://adventuresinsecurity.com/Papers/Build_a_Security_Awarsseness_Program.pdf

Patton, M.Q. (2002). Qualitative Research and Evaluation Methods.Thousand Oaks, CA: Sage.

Post, G. V., & Kagan, A. (2007). Evaluating Information Security Tradeoffs: Restricting Access Can Interfere With User Tasks. *Computers and Security*, 26 (3), 229 - 237.

PricewaterhouseCoopers (2012). Changing the Game: Key Findings from the Global State of Information Security Survey 2013. Retrieved February 21, 2013, from http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf

Reardon, M. (2007). Smartphones Sales Skyrocket. Retrieved December 31, 2012, from http://news.cnet.com/8301-10784_3-9816072-7.html

Restine, K. A. (1999). How Beliefs About Teaching and Learning Influence the Technology Training Experience: An Explanatory Case Study. Unpublished doctoral dissertation, Oklahoma State University, Stillwater.

Rouse, W.B., & Baba, M.L. (2006). Enterprise Transformation. *Communications of the ACM*, 49(7), 67–72.

Sacco, A. (2007). Study: Average Value of Business Info on Travellers' Laptops Equals $525K. Retrieved November 06, 2012, from http://www.cio.com/article/147000/Study_Average_Value_of_Business_Info_on_Travelers_Laptops_Equals_525K

Sale, N. (2007). The Way We Will All Work. *Global Telecoms Business*, 93, 66 - 67.

Schlienger, T. & Teufel, S. (2003). Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture", *Database and Expert Systems Applications conference proceedings* ,14, 405-409

Schilling, J. (2006). On the Pragmatics of Qualitative Assessment: Designing the Process for Content Analysis. *European Journal of Psychological Assessment*, 22(1), 28-37.

Schlienger, T., & Teufel, S. (2002). Information Security Culture: The Socio-Cultural Dimension in Information Security. *Management, Proc. Of IFIP TC11 17th International Conference on Information Security (SEC2002), IFIP Conference Proceedings* 214, 191-202

Scott, J.E. (2007). Mobility, Business Process Management, Software Sourcing, and Maturity Model Trends: Propositions for the IS Organisation of the Future. *Information Systems Management*, 24, 139–145.

SecurityWeek News. (2011). Multiple Variants of Android Malware "Hong Tou Tou" Surface in China | SecurityWeek.Com. Retrieved March 17, 2013, from http://www.securityweek.com/multiple-variants-android-virus-hong-tou-tou-surface-china#

Seybold, A.M. (2008). The Convergence of Wireless, Mobile, and the Internet and its Relevance to Enterprises. *Information Knowledge Systems Management*, 7, 11–23.

Sheller, M., & Urry, J. (2006). The New Mobilities Paradigm. *Environment and Planning, 38*(2), 207–226.

Smith, H.W. (1975). Strategies of Social Research : The Methodological Imagination. Englewood Cliffs, NJ: Prentice-Hall.

Spender, J. C. (1996). Organizational Knowledge, learning and Memory: Three Concepts in Search of a Theory. *Organizational Change Management*, 9(1), 63-78

Stallings, W. (2003). Network Security Essentials (Applications and Standards). Second Edition. Pearson Education. ISBN 0-13-035128-8

Standards South Africa (2005). SANS 17799:2005. Pretoria: Standards South Africa.

Stemler, Steve (2001). An overview of content analysis. Practical Assessment, Research & Evaluation, 7(17). Retrieved April 24, 2013 from http://PAREonline.net/getvn.asp?v=7&n=17

Streubert, H. J., & Carpenter, D. R. (1999). Qualitative Research in Nursing, Advancing the Humanistic Imperative. 2nd Edition. Philadelphia, PA: Lippincott

Takesue, M. (2007). Emerging Security Information, Systems, and Technologies. *SecureWare*

Taflinger, R. F. (1996). Introduction to Research. Retrieved November 05, 2012, from http://public.wsu.edu/~taflinge/research.html

TechAmerica (2012). Fiscal constraints and future challenges: Driving innovation at the CIO level. *22nd Annual Survey of Federal Chief Information Officers,* Retrieved February 21, 2013, from http://www.federalciosurvey.com/

Urry, J. (2007). *Mobilities*. Cambridge: Polity Press.

U.S. General Accounting Office (1996). Content Analysis: A Methodology for Structuring and Analyzing Written Material. GAO/PEMD-10.3.1. Washington, D.C.

VARBusiness (2006). Mobile Users Pursue Risky Business. *VARBusiness*, 22 (22), 51.

Verge Staff (2012). How to Buy a Smartphone: A Guide. Retrieved April 28, 2013, from http://www.theverge.com/2011/11/16/2565102/smartphone-buyers-guide#

Walker, G. H., Stanton, N. A., Salmon, P. M., & Jenkins, D. P. (2008). A Review of Sociotechnical Systems Theory: A Classic Concept for New Command and Control Paradigms. *Theoretical Issues in Ergonomics Science, 9*(6), 479–499.

Walters, P. (2012). *The Risks of Using Portable Devices*. Carnegie Mellon University. US CERT. Retrieved November 05, 2012, from http://www.us-cert.gov/reading_room/RisksOfPortableDevices.pdf

Walton, R. E. (1985). From control to commitment in the workplace. *Harvard Business Review, 63*(2), 77-84.

Waterson, P. E., Gray, M. T. O., & Clegg, C. W. (2002). A sociotechnical method for designing work systems. *Human Factors*, 44(3), 376-391.

Weber, R. P. (1990). Basic Content Analysis, 2nd ed. Newbury Park, CA.

Webster, J. & Watson, R., T., (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26 (2), 13–23

Whitman, M. E. & Mattord, H. J. (2004). *Management of Information Security*. Thompson Course Technology

Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security* (4th Ed.).

Wilson, J. R. (2000). Fundamentals of ergonomics in theory and practice. *Applied Ergonomics*, 31, 557-567.

Woo, D. M., & Vicente, K. J. (2003). Sociotechnical systems, risk management, and public health: comparing the North Battleford and Walkerton outbreaks. *Reliability Engineering and System Safety*, 80, 253-269.

Yuan, Y., Archer, N., Connelly, C.E., & Zheng, W. (2010). Identifying the Ideal Fit between Mobile Work and Mobile Work Support. *Information & Management*, 47(3), 125–137.

Zhang, Y., & Wildemuth, B. M., (2009). Qualitative Analysis of Content. *Applications of Social Research Methods to Questions in Information and Library Science*, 308-319.

APPENDICES

APPENDIX A

Interview Questions

Work and Mobility Related Questions

1. Can you tell me a little bit about yourself and your organization?

2. What are your roles and responsibilities within the organization?

3. How mobile are you at work? Explain.

4. Do you travel on work related duties?
   4a. How often?

5. During travel times how do you get business related emails and messages across on time.

6. How often do you access your organizations data resources with your Smartphone when you are in public places like the airport?

General Questions about the Smartphones

7. Which type/brand of smartphone do you own?

8. What activities do you use your smartphone for? Personal or work related activities? Explain.

9. What do you think about using smartphones as working tools?

10. Have you ever thought about the implications of using your smartphone (either BYOD smartphone or company assigned smartphone) for work related purposes? Describe

11. Which do you think should be used for work purposes; BYOD smartphones or company assigned smartphones?
    11b. Why?

Smartphones Security

12. Do you think organizations must have a mechanism to secure portable devices including smartphones whether BYOD or company assigned smartphone? Why?

13. Do you open company related files on your smartphone?
    13a. How often?
    13b. Why?

14. Do you store company files on your smartphone?

15. How do you connect to the organization's data resources from your smartphone?

16. Describe the security settings or configurations you have on your smartphone.

17. Do you think antivirus should be used on a smartphone? Explain.

18. Do you have a mechanism to wipe out data if you smartphone is lost or stolen? Describe.

19. How do you know if your device has been compromised? Describe.

20. How do you secure your smartphone's external memory card? Describe.

Applications

21. What do you think about installing additional application such as email readers, games and music players etc. on your smartphone?

22. How do you install application on your smartphone, through the app store or through another means?

23. How do you know software you have decided to install on your smartphone is or is not malware? Describe

Policy Related Questions

24. Does the company you work for have smartphone usage policy? Can you please describe if possible?

25. How does this policy facilitate or impede work especially via a smartphone? Describe.

Concluding Questions

26. What recommendations can you make regarding the use of smartphones as working tools to make them more productive and less prone to risks?

27. Do you have anything else to share?

Thank you for your time!!!

APPENDIX B

Interview Schedule

No.	**Name of Participant**	**Date of Interview**	**Time of Interview**	**Duration of Interview**
1	Participant 1	4th April, 2013	Thursday 12:00 CET	23 Minutes
2	Participant 2	4th April,2013	Thursday 15:00 CET	37 Minutes
3	Participant 3	5th April,2013	Friday 10:00 CET	20 Minutes
4	Participant 4	5th April, 2013	Friday 11:00 CET	20 Minutes
5	Participant 5	5th April, 2013	Friday 13:00 CET	15 Minutes
6	Participant 6	5th April,2013	Friday 14:00 CET	26 Minutes
7	Participant 7	8th April, 2013	Monday 10:30 CET	20 Minutes