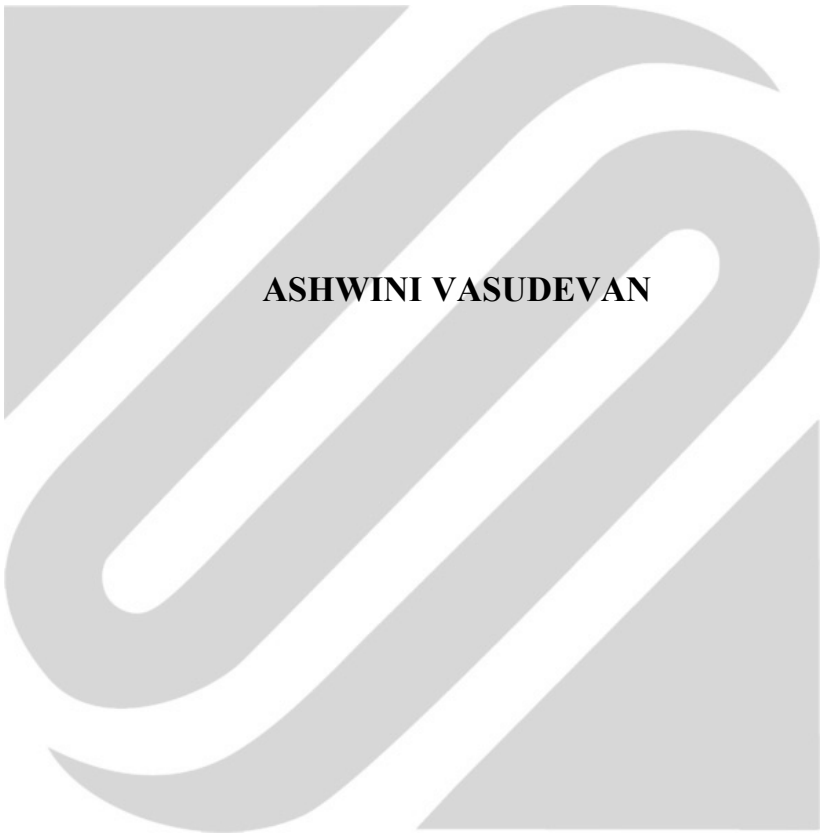
BUSINESS PLAN
BRING YOUR OWN DEVICE (BYOD)



ASHWINI VASUDEVAN

AN INDEPENDENT STUDY SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE GRADUATE SCHOOL
STAMFORD INTERNATIONAL UNIVERSITY
MASTER OF BUSINESS ADMINISTRATION
ACADEMIC YEAR 2014

BUSINESS PLAN
BRING YOUR OWN DEVICE (BYOD)

ASHWINI VASUDEVAN

AN INDEPENDENT STUDY SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE GRADUATE SCHOOL
STAMFORD INTERNATIONAL UNIVERSITY
MASTER OF BUSINESS ADMINISTRATION
ACADEMIC YEAR 2014

The Research has been approved by

Stamford International University

The Graduate School

Title: Bring Your Own Device Threats, Risks

Researcher: Ashwini Vasudevan

The Independent Study Committee:

Advisor .....

(Dr. Dolly Samson)

Committee Member .....

(Dr. Martin Goerlich)

Committee Member .....

(Dr. Donn pjongluck)

.....

(Mr. Adam Tyler Thompson)

Asst. President, Academic Affairs &

Dean of Business and Technology

6th December, 2014

Title: Bring Your Own Device Threats, Risks

Researcher: Ashwini Vasudevan **Student ID**: 0112430004

Degree: Master of Business Administration

Advisors: Dr. Dolly Samson

Academic year: 2014

Today's world is characterized by a heavy dependence on information technology and technological devices to perform even the simplest of tasks. 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. It also explains employees comfort zone in using their Own PDA's rather than the computers provided by the organization.

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. Due to the mobile nature of the device, it has brought challenges to the needs of organizations. As the sale of PDAs continue to increase so does the number of vulnerabilities on mobile operating systems. Knowing where to place the PDAs 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?

ACKNOWLEDGMENT

I am very pleased to present my research work which I have collected information from various sources and conducted the study to complete. The successful completion of this study is the outcome of the contribution of a number of people to whom I'm grateful and thank them from the very deep of my heart. So, I would like to take this opportunity to thank all those people who helped me in preparing this research paper. First of all I would like to express my great respect to almighty for providing me the strength and energy to prepare this paper.

I would like to pay my gratitude to our respectable Dean of Graduate School Dr. Apitep Saekow who has given me the opportunity of doing this research paper.

Then I would like to thank my respected advisor Dr. Dolly Samson who provided me very much valuable information, which was very mandatory for me to complete this research paper. Her advice and assistance proved to be of great benefit to my research for the correction and completion of this work.

I would also like to give special thanks to our friends and seniors, who helped to complete this report.

Here and now, I would like to take this opportunity to express my gratitude and highest regards for both, and sincerely thank them for their kindness.

Ashwini Vasudevan

CONTENTS

CONTENTS(Contd.)

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

CHAPTER 1
INTRODUCTION

The usage of mobile devices has increased dramatically during the last decade and has grown significantly in the business sector as well as the private sector, where the majority of citizens in first-world countries depend on smartphones in their daily life. Since the introduction of smartphones into the workplace, the perimeter have expanded and allows work to be conducted from the outside of the workplace. Some companies require their employees to be more flexible in their work, which can require them to be able to access their email, calendar and other company data remotely. The market is reporting of a trend where employees would prefer to use their private devices for work-related activities instead of company-owned devices and this phenomenon is discussed under the term: Bring Your Own Device.

BYOD refers to a concept where employees are allowed to use their private devices (laptops, smartphones, tablets etc.) for work - to carry out work-related tasks and gain access to internal company resources. It offers more freedom and flexibility for the employees and cuts maintenance- and support costs for companies. Since the employees are responsibility for the devices then companies can primarily focus on the safety of their data. However, this is not an easy task since one of the biggest challenges with BYOD is to prevent data leakage and is mainly due to the lack of control over the devices from an enterprise perspective. According to a 2011 Trend Micro report, users prefer to use their own personal devices in the workplace because they are (a) easier to use, (b) more convenient, and (c) allow them to mix their personal and work-related information (Garlati, 2011).

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).

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.

Policy development, one of the goals of this study is to identify a set of factors that can be used to guide the development of policies that address the consumerization of IT throughout an organization (International Data Corporation, 2011). Factors for policy development may include how to manage (a) authorized use, (b) prohibited use, (c) systems management, (d) policy violations, (e) policy review, and (f) limitations of liability (Green, 2007). BYOD In Microsoft

1.2 Statement of the problem

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 corporate 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, tablets 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 an increase in the use of the BYOD 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.

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), employees use smartphones 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 remains at a lower rate compared to how fast mobile technologies are growing (PricewaterhouseCoopers, 2012).

1.3 Purpose / Objectives

Figure 1.1 BYOD Analysis

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 BYOD 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 BYOD when used for work in the organization under study.

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 BYOD 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 BYOD within an organization.

iii. Study countermeasures that could facilitate relatively threat free working environment even with the use of BYOD.

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 BYOD as working tools?

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

R.Q.3: How is the comfort zone of the employees?

This study outlines some of the current threats, risks and vulnerabilities associated with the use of BYOD and the most significant threat and risk areas of the BYOD. It also outlines the perception of BYOD users with regards to information security. Lastly, the study analyzes the effect of mobility and BYOD usage on an organization's information security. Since workers in an organization use different BYOD that run different operating systems; IOS, Android, Symbian or windows; the aim of the study is not to target any particular operating system. The BYOD 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.

This study has several limitations that may affect its transferability. The study was limited to five organizations using the BYOD concept. The employee's experiences and attitudes cannot represent all the possible scenarios of using the BYOD for work especially because the organization in question is not one that produces so much confidential data.

1.5 Significance

According to a 2011 International Data Corporation (IDC) study on the consumerization of IT, 40.7% of the devices used by information workers to access business applications are personally owned, an increase of 10% over 2010 (Burt, 2011). The ongoing use of personally owned mobile devices in the workplace is forecasted to continue to grow. According to Cisco Systems' annual Visual Networking Index Forecast released in June 2011, by 2015, "there will be almost 15 billion network connected devices, including smart phones, notebooks, tablets, and other smart machines, translating to more than two devices for every person on the planet" (Burt, 2011, p.30). The ongoing IT industry welcomes the BYOD concept in a effective way to reach effective results.

Bring Your Own Device (BYOD)

A term used to refer to the trend of bringing a personally owned mobile device to the workplace for use and connectivity on an institutional network (International Data Corporation, 2011).

Mobile Device – A handheld computing device that can be used from multiple locations. Examples include basic phones, portable media players, and smartphones (Crisp &Williams, 2009).

Mobile Device Management (MDM) – Software designed to securely manage mobile devices used across an enterprise (Trend Micro, 2012).

Operating system – A software program that manages computer hardware resources and provides services for application software (Kim, 2011).

Short Message Service (SMS) – A text messaging service of mobile communications systems using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile line devices (Motiwalla, 2007).

Smartphone – A fully featured mobile telephone with personal computer-like functionality (Green, 2007).

Tablet – A mobile computer integrated into a multi-touch screen and operated by touching the screen rather than using a physical keyboard and mouse (Burt, 2011).

Telecommunication Carrier – A provider of telecommunications services (Kim, 2011)

CHAPTER 2
LITERATURE REVIEWS

Two trends have been major causes of the BYOD phenomenon. The first trend is from a company perspective. Companies want to reduce complexity and cost of managing mobility. The second trend is from the employer perspective. Employees want to use the most popular devices that they use as consumers, instead of the device provided by their employer.

BYOD is enabling workers to use their own device for both work and personal purposes. The main characteristic of BYOD is that this strategy is completely device agnostic. It does not matter anymore on which operating system you want to work or on which device you want to work. BYOD will make sure that your work environment is accessible.

There are a few different ways for a company to adopt the BYOD strategy. The level of support is the most interesting characteristic that varies. A company can choose to give support to people's own devices, but this will be a great challenge for the IT support. Instead of knowing their way around a couple of models, they need to know more about different operating systems, different smartphone models, different laptop models etc. On the other hand a company can give no support to people's own devices. This will reduce support costs, but on the other hand when a smartphone or laptop is not functioning correctly the owner is not able to do his or hers work. So there are other costs incurring. The other important enabler for a good BYOD strategy is the development of device agnostic applications. Reading and answering emails is very simple to accomplish on your own device, but the hard part are the specific business applications. These applications must be often be developed. It highlights the need for organizational information security and the pressure that management and employees put on security components as they attempt to maximize efficiency and minimize workload.

2.1 Organizational 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.

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 (Furnellet al., 2006; Takesue, 2007; Botha et al., 2009; Allam, 2011).

2.2 Smartphones Risks

Whitman and Mattord (2004) define a risk as a product of the likelihood of a vulnerability tobe 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.

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.

2.3 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.

2.4 BYOD

Table:2.1 BYODs

xYOD Type	**Distinction**	**Hardware owner**	**Who contracts for service**	**Who pays for service**
"Bring" YOD (BYOD)	Personal device	End user	End user	End user
				organization
				shared
"Here is" YOD (HYOD)	Multiple mobile devices available but assigned based on user's role	Corporation	Corporation	Organization
				Shared
"choose" YOD (CYOD)	Users given a choice of "selective" devices	Corporation	Corporation	Organization
				Shared
			End user	End user
				Shared

This use of an employee-owned mobile device in the workplace differs from the use of a corporately-provided mobile device, in two ways. The first is ownership. Whereas a corporately provided mobile device is owned by the organization that issues it, a BYOD device — what we will refer to as a BYOD — is owned by the employee.

This difference in ownership results in a difference in usages between the two kinds of devices. Because a corporately-provided mobile device is owned by the organization, there is likely to be a policy in place that forbids or severely restricts non-work-related uses. On the other hand, because a BYOD is owned by the employee and not the organization he or she works for, one may assume, if not explicitly stated in a policy, that the employee will be using the device for personal, non-work-related purposes in addition to work. Second, this situation of BYOD, where a device is used for both personal and work purposes, means that two kinds of personal information will flow through the device, both of which will require proper protection on the part of the organization that employs the individual using a BYOD. On the one hand, the device will most likely process and have access to the personal information of the clients of the organization, i.e., those individuals with whom the organization has interacted and from whom it has legitimately collected and used personal information. On the other hand, the device will also most likely process and contain personal information about the employee to whom the device belongs as well as perhaps close associates of the employee, e.g. Significant others, family members, friends, etc.

2.5 Privacy and Information Security Risks

An organization has an obligation to protect the personal information it has collected for legitimate purposes from unintended uses or disclosures, regardless of who owns the device used to process a client's personal information. With BYOD, an organization has less control over the devices used to process clients' personal information than in the case of corporately-owned and issued mobile devices. For example, with BYOD an organization typically has less control over:

The kind of device, e.g., smartphone, tablet, laptop, etc.

The make and model of the device;

The operating system and applications installed on the device;

The purposes for which the device is used;

Where and when the device is used; and

Who uses the device?

An overview and description of common risks to organizations associated with BYOD uses are provided in the table below. Risks in bold font are of particular

relevance to this paper. In addition, significant risks fall upon individual clients and employees as a consequence of an organization's poor management and control of personal information. All risks must be identified, acknowledged, measured and assessed, prioritized, and mitigated through an organization's systematic application of PbD principles, a comprehensive security program, and an appropriate mobile device management strategy, as outlined below

Table 2.2: Common BYOD Risks to Organizations

Risk type	Risk	Description
Internal	Employees can be dissatisfied by the limited selection of supported devices	Employees favor flexibility and minimal restrictions on device use
	Organizations may be exposed to liability concerns arising from device usage or implications posed by reimbursements you provide to employees	Where and when devices are used could shift liability ownership to your organization, for example, employees working onsite, who lose their phone or have them damaged, may be entitled to full device replacement paid for by the employee
	Supporting too many devices and inefficient support processes can result in incremental costs	Devices are consumer-focused, have limited 'out-of-the-box' security, and come in a variety of different platforms and makes, which inhibits IT's ability to manage and control devices
	Undisciplined use of devices by employees can expose your organization to additional security threats	The consumerization of devices and resulting advancement of applications, app stores, data portability (e.g. on the cloud), etc., promote user behavior that can be incongruent with what's ultimately best for your organization

Table 2.2: Common BYOD Risks to Organizations (Cont.)

Risk type	Risk	Description
External	Competitors may possess productivity advantages if your BYOD program is not appropriately defined and executed	A BYOD program that contains high degree of control on device usage, platforms, and applications can impede potential productivity gains and ultimately result in competitive risks for your business
	Your organization may be exposed to regulatory risks that result from data breaches, information loss, etc	Privacy issues are top of mind in today's business world, as organizations are increasingly accumulating and exploiting personal Information. Compromising an employee's personal Information can lead to severe consequences for your organization.
	BYOD policies may infringe on employee rights, such as requirements for overtime pay	Employees that are participating in BYOD, and are contacted outside of normal working hours for work purposes, may be entitled to overtime pay
	Increasing level of device diversity and complexity may stress your abilities to manage these devices	Proliferation of multiple devices and platforms (as the result of consumerization) minimizes the feasibility of a simple and single solution to device management. Your organization, facing Significant hurdles in effectively managing devices, may incur unforeseen costs and be exposed to security concerns.

2.6 Privacy-Aware Mobility Strategy

A privacy-aware strategy that considers the needs of the employee and the organization is required to ensure that the use of new and powerful mobile devices is possible, while at the same time protecting both the employee and the organization. The following checklist will provide a starting point from which to evaluate readiness and capabilities for a privacy-aware BYOD program

Table 2.3: Readiness/Capability Checklist

#	**Control**	**Description**
1.	Acceptable Use Policy	Clear and concise definitions and statements of what is allowable on the device, once access to organizational data is permitted. Additionally, this can guide the behavior of employees, such as incident response personnel and IT teams when dealing with personal devices
2.	Privacy policy	Inclusive of mobile device use and behavior expected from both employees and third parties acting on behalf of the organization
3.	Statement of location of use	Where the devices are expected to be used
4.	Decision on operation model for Mobile Device Management(MDM)-Internal versus outsourced	This will impact who has access to corporate data and personal data
5.	Decision on mobile device camera use Data classification and Control	Statement of where and when the camera capabilities of the device are permitted. This can be enforced technically via MDM technologies.
6.	extending it to mobile device use	Absolutely critical statement as to the sensitivity of the organizational data that will be permitted on the device. It is conceivable that restricted data should never land on a mobile device

Table 2.3: Readiness/Capability Checklist (Cont.)

#	Control	Description
7.	Consideration of Android solutions such as SE Linux, Samsung KNOX, Cisco Any Connect, Aruba Workspaces, etc.	Recent announcements of elevated security solutions for Android need to be proven in pilot deployments. Where they are successful, they provide strong separation of personal and corporate data

The Review of Literature ends with a Conclusion that clearly states that, based on the review of the literature, the gap in the knowledge that is the subject of the study has not been studied. Remember that a "summary" is different from a "conclusion." A Summary, the final main section, introduces the next chapter.

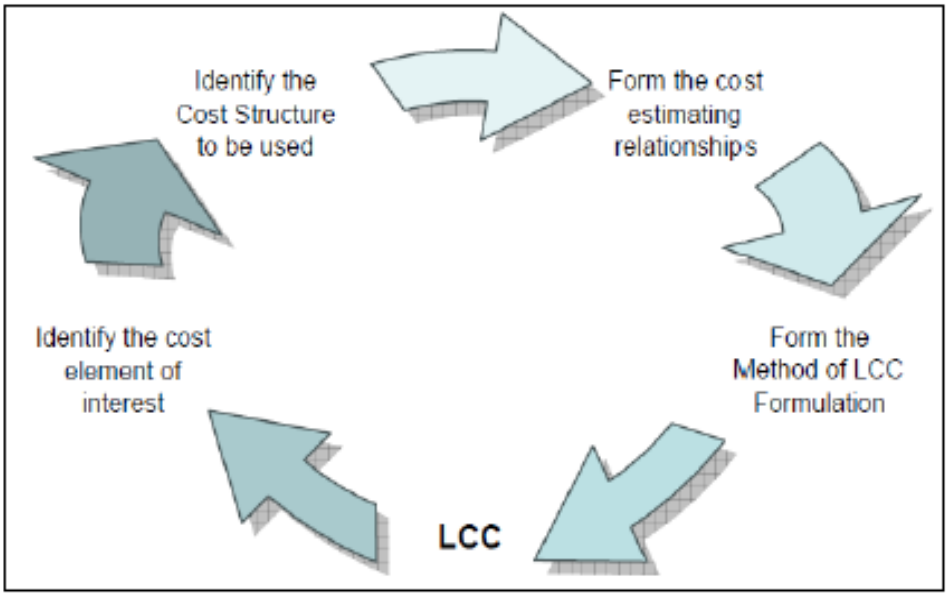


Figure 1.2 Life-Circle costing procedure

Source: Adopted from Wang, 2004

CHAPTER 3
RESEARCH METHODOLOGY

3.1 Research Method

This study focuses on implementation BYOD used in five different organizations. This study will be conducted by qualitative research method extracting information regarding security, risks, privacy, policy. In case of this study qualitative methods would be more significant because of its ability to provide complex textual descriptions of how people experience a given research issue.

The qualitative method used here is in-depth interview, observation, focus groups. Within these three methods for this study will be conducted by in depth interviews or it's called individual interviews.

3.2 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;

1. Planning. E.g. identifying the sample and the type of data to be gathered.

2. 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.

3. Collecting the data,

4. Analyzing the data. E.g. transcribing and/or reviewing the data collected through the interviews and finally

5. 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 PDA users on how secure or insecure the use of PDA 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 employees in a company based of the researcher's judgement. The interview protocol is attached as appendix A.

3.3 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 employees of the company.

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 8 mails sent on the 20th October, 2014, 5 obliged. On the 1st

November of 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 process I got to meet 2 people in person and know about the company and the information required. All five were done in 5 days. 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.

3.4 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:

1. Work and mobility
2. General PDA knowledge
3. PDA security
4. Applications installation and
4. 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:

1. Set the tone of the interview
2. Establish rapport with the participant
3. Discuss the significance and format of the research
4. Allow participants to ask questions before we started and

5. 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.

3.5 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 dan from interviews were analizad in order to provide país of discernían, examinan, comparan and contra Sting, and interpretan 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 PDA's 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.

3.6 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 analysis. 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.

The use of qualitative content analysis in analyzing 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. Inductiva 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.

3.7 Types of Content Analysis

1. Conventional Content Analysis

The study starts with Observation- Helps to code categories directly and inductively from the raw data. This approach is useful for grounded theory development.

2. Directed Content Analysis

The study starts with Theory- Initial coding starts with a theory or relevant research findings. During data analysis, the researchers immerse themselves in the dataand allow themes to emerge from the data. The purpose of this approach usually is to validate or extend a conceptual framework or theory.

3. Summative Content Analysis

The study starts with 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.

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:

1. Work and Mobility
2. General Questions about the PDA's
3. PDA's Security
4. Applications and
5. 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

1. 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

2. 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 comparisons.

Table 3.1: shows a snippet of the code manual.

Category name	**Definitions**	**Examples**	**Coding rules**
C1: Employee Mobility	To be considered a mobile worker one must be an fall under one or more of the following, 1. Employee who uses ICT to access remote information from their home base, workplace, in transit, and at other Destinations. 2. Employee who is free from the spatial and/or Temporal constraints of the traditional office. 3. 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.	1.The employees who often travel once a week 2. Employees who go for conferences and workshops 3 to 7 times a year 3. The employees who can respond from their own smart phones through mails. 4. The employees who have to work in two working stations can schedule their meetings accordingly.	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, 1. To make and receive work related calls. 2. To read and reply to emails.	I use my smart phone only for reading and responding to emails and making and receiving calls 1. When employee need an app for work I install it and use it.	All examples indicate that the employee uses The device for work.

Table 3.1: shows a snippet of the code manual (Cont,.)

Category name	**Definitions**	**Examples**	**Coding rules**
C2: Accessing Organizational Resources	3. To save a contact list for work. 4. To have a schedule for work purposes. 5. To install apps for work.To access other organizational resources via the internet.	2. Employee have a contact list on my work assigned smartphone. 3. Employee 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.

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 under sight. 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.

3.8 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 seminars 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 4
RESEARCH 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.

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

Numerous threats, risks, and/or vulnerabilities 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. Some of the smartphones have the facility where they can transfer data just by tapping on with the other phone. This would lead to great threat of information theft. Some people do not care to put any screen lock or pins for their devices, which again leads to information theft and risk of leakage of information. Pins and patterns on mobile phones can also lead to risk factors, which again can be easily observed by other persons and can apply the pin and pattern to take needed information.

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 did not 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 themfor 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.

4.1.1 Work and Mobility

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 workerwho 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.

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 preferto 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 behavior are one or all of the under listed:

1. It is hard to use the small phone interface, or

2. That there is more security on their computers than there is on their phone or

3. That the cost of using the smartphone is higher in term of charges than it is on computers.

4.1.2 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 is 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 did not 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 did not 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. 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 a colleague or someone who had experienced huge costs of roaming mobile data charges had told this to them. To them using roaming mobile data was more damaging than any other risks, 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. However, using the smartphone provides a cost effective way of making and receiving calls, reading and replying to emails and managing work related schedules, if the user does not control it carefully and intentionally things could get out of hand and

confidential data transferred via emails or phone conversations could get into the wrong hands.

4.1.3 Other PDA's

Respondents find it very easy to use other PDA more safely and find it less risky than using a small screen smartphones. It has wider screen and advanced security options like firewalls, VPN, best antivirus software provided by the company. To fail brute-force attempts to compromise device credentials, the company has insisted the employees on changing all user credentials every 4 weeks after which the credentials expire and it becomes necessary for the employee to register new credentials to continue using the device.

4.1.4 PDA Security

To be able to regulate and improve security via PDA it is the duty of the organization to assign PDA 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 PDA that had been assigned to them as Furnell et al. (2006) spoke about. They believed that when a company assigned PDA, 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 PDA; 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 PDA 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 PDA for maximum benefits. Having a PDA usage policy will make employees aware of the potential risks of using PDA for work purposes. It will also make them aware of what they can and cannot do with their company assigned PDA.

It is not surprising to see employees use BYOD's in addition to the company assigned PDA. Respondents in this study had an additional PDA for their personal use. In order to keep a high standard of information security, applications that the organization does not support must be disabled in its environs. One intelligent feature can be that company assigned PDA 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 PDA. 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 PDA to share data with another

PDA when they come into close contact with each other if not put off could cause the PDA to share data without the user's knowledge. The organization must make a conscious effort to block services that they do not 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 PDA. 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 PDA. 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.

On the topic on using anti viruses on PDAs, respondents' did not know such existed and so did not have any. The apple brand PDA users suggested once more that their apps were secure and so did not 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 PDA. Again, they were aware that PDA had a mechanism to wipe out data when they were stolen but had not configured this yet.

4.1.5 Application Installation on Company Assigned PDA

With the issue of installing additional application on the PDA, respondents said that they did not do this on the company assigned PDA except it was needed to do their work. They said though that they installed applications such as news readers on the work assigned PDA 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 PDA as well as highlights on recent happenings with the PDA 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 PDA. The most important aspect to the respondents was that once, it did not go against organization policy; they did not 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 PDA. 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 PDA 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. 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. However, 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 PDA.

4.1.6 Information Security Policy on the Use of PDA

A policy spells out a set of organizational guidelines that describe acceptable and unacceptable behavior of employees within the workplace. It was surprising to know that the respondents did not know what exactly the PDA usage policy stated. While they were aware of a phone usage policy in place that disallowed making private calls on the work assigned PDA 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 PDA 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 PDA when employees travelled outside the country. The smart aspects of the PDA 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 PDA 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 PDA. Indeed there may not be anything special that needs to be protected on the PDA, 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 they will always would have access to the PDA 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 PDA 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 unauthorized 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 PDA 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 centered, these policies must be updated to meet the new need.

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

The first approach to minimizing the threats, risks, and/or vulnerabilities associated with the use of PDA as working tools is with 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 PDA 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' PDA. If certain applications must not be used or are not allowed on the company assigned PDA, 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 PDA that has internet connection on it. Policy says that no roaming while abroad. However, 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 does not 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), Schlienger, and Teufel (2003) must be cultivated in the organization as these mould the attitudes and behavior 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 PDA and other portable devices safely and especially for optimal security. Only applications that are supported by the organization should be allowed on company assigned PDAs while BYOD PDAs 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 do not 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 unauthorized employees and especially via

unauthorized devices such as BYOD's. The network could also be segmented so that areas that are accessible to employees via their PDA 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 shareholders have in them about their data.

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

1. Protect the PDA physically and disallow others from using it.
2. Backup your personal data from time to time.
3. Be careful when you Wi-Fi as not all Wi-Fi are secured.
4. Browse wisely choosing only secured sites that support encryption especially when there is the need to exchange sensitive information.
5. Clear your cache.
6. Have a data wiping mechanism installed on the PDA.
7. 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.
8. Check all permissions assigned to any app you want to install before they are installed.
9. Don't throw or give away your PDA without wiping all the data you have on it.
10. Encrypt data on the device as well as data on any removable memory that the phone uses.
11. Update your PDAs OS as soon as it is released.

4.3 HOW IS THE COMFORT ZONE OF EMPLOYEES

Most of the employees seem to be in a very comfort zone using their own PDA in the organization. The employees find to be less stressful as far as they have their own device in hand to work from anywhere. They can work on any time scheduling their own project accordingly from home or at office connecting to a single database. Some employees prefer work from home more comfortable than work station with their

own device. Employees get their own space to work and produce the best results effectively. They can schedule their meeting whenever and reschedule by just updating in the common portal. Employees tend to update their work easily from anywhere. Most employees are satisfied working with their own device. However, some employees find it difficult using the small screen PDA's with threat to information theft.

CHAPTER 5
SUMMARY, CONCLUSION & RECOMMENDATION

5.1 Summary

Analyzing the data gathered and literature review has helped us to find apparent threats, risks and consequences regarding the use of PDA's in an organization. These chapter portraits the summary of threats, risks, vulnerabilities and information security with use of PDA's in an Organization.

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. There were instances where Bluetooth had been left opened without the user knowing. How do we achieve competitive advantage and create conditions for the success of our organization if the device that can lead people into our mailbox where confidential matters are discussed, is left unprotected? Users were not aware that expandable memory chips could support encryption or that anti-viruses 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.

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 PDA enter authentication details occasionally as they believe the PDA is personal and is used by them alone. Users of the PDA move about within the organization as well as outside the organization. While on holidays, some employees carry the device along. Be it a personal PDA or an organization owned PDA the device is used to access open Wi-Fi as the user travels around. Not all these hot spots can be trusted. Scrupulous people who are sniffing around for any confidential data they can lay their hands on own some of these open connections. 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 PDA 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 PDA for both work purposes and personal purposes imply a possible breach of the confidentiality, availability and integrity of the organizational data resources (Fitzgerald, 2009).

Some users were not aware of the antivirus programs installed and their best uses. Some found it very annoying because each time they will have to go through a tedious task before entering the organization portal. 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 has 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. Some applications in the smartphones reveal the location services unintentionally. 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).

5.1 Information security on mobility of PDA's

Information Security gives an assurance that information risks, 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). 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 tablets, ipads, smartphones, laptops.

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.

PDAs, 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. 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. 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.

PDA's 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.

As the users move around, the apps that they have installed on their PDA's 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.

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 PDA's 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 PDA's 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 PDA's 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 PDA's then undesired modification of information cannot also be assured. If PDA's 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.

5.2 Threat and Risks

Smartphone threats are diverse. 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. The perception of users on the risks of using a PDA's 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. 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.

5.3 Countermeasures

There are numerous counter measures that can be employed when embarking on PDA 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.

5.4 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.

One qualitative study cannot explain every possible scenario of what can happen when PDA's 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 PDA's as working tools.

A practical experimental setup to investigate the security of the different PDA's operating systems as we have today and how susceptible they are to mobility and information security

5.5 Findings

The BYOD is a great boon to the organization in terms of Employees satisfaction, profit for the Organization, there by increasing the over all profit. The work is Flexible, work at anytime and anywhere. For the above Research done, the samples were gathered from different organization, persons employed at different positions. The findings were taken from two countries, Thailand and India. Comparing both the countries, the satisfaction level, awareness of this technology, acceptance of BYOD in organization, varies drastically between these two countries. In Thailand, the acceptance of BYOD is on a higher rate. The Employees and the organization are on the verge to transform this into action and many companies have already implemented this, though there are many security threats. In India, the Technology is yet to take boom. Organizations are aware of this concept, but they are reluctant due to security and data threats. Very few companies have made this into action in India. The satisfactory level of Employees remains the same as Thailand. Awareness of this concept in India yet to boom. The Samples were taken from different organization and from different positions. Organization tend to follow this BYOD concept to the Employees, who are in higher positions, because they would have better knowledge how to secure the data from threats with more responsibility.

REFERENCES

1Ahmed, 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, StJohn'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/ socio technicaltheory.htm

Allam, S. A. (2009*). A model to measure the maturity of Smartphones security at softwareconsultancies'*, 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-appsmalware?cat=technology&type=article#

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.

REFERENCES (Cont.)

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. *InformationKnowledge 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.

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.

REFERENCES (Cont.)

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-bycharlatan-vendors-says-google-engineer/

Dunning, J. P. (2010). Taming the Blue Beast: A Survey of Bluetooth Based Threats. *IEEESecurity & 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 December31,2012,from http://www.techworld.com/mobility/features/index.cfm?featureid=3204

REFERENCES (Cont.)

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

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 side loaded 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 SystemsManagement*, 7 (1–2), 77–97.

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

REFERENCES (Cont.)

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 Fraudand 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.htmJuniper Networks (2011). Mobile Device Security, Emerging Threats And EssentialStrategies - Key Capabilities For Safeguarding Mobile Devices And Corporate Assets. Whitepaper, Juniper Networks, Inc.

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

Kisling, E. L. (2006). An implementation of information technological change: A sociotechnical 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. NewburyPark, 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

REFERENCES (Cont.)

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 TheoryModels. *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 Assuranceand Security*, 306–310.

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

APPENDIX A
SURVEY QUESTIONNAIRE

Mail of Consent

Byod

Researcher's Name and Contact Information

Ashwini Vasudevan (ashwini.v@stamford.edu)

Supervisor's Name and Contact Information

Dr.Dolly Samson (dolly@stamford.edu)

Dear Valued Participant,

You are being requested to take part in a research project. Before you decide to participate, it is important for you to understand why the research is being conducted and what it will involve.

Interviews will be last for about forty five minutes at any time of your choice. The researcher will make audio record this interview only with your permission. A copy of transcript can be sent to you to confirm the accuracy of our conversation. Answering some question about self-opinion might cause transitory embarrassment. So you are completely free to refuse to answer any question and have the right to stop tape recording at any point in the conversation. The researcher will comply with the regulation of the university to protect the privacy and the rights of the research participants.

Are you interested in receiving a copy of final results of IS? If yes then please contact with the researcher by the above email address.

Thank you very much for sharing your valuable time and kind assistance.

APPENDIX B

Survey Questionnaire

1) Tell me about your organization.
2) What kind of devices are used in your company.
3) How mobile are you at work?
4) Comfortable level using the device
5) What are the security risks overcome
6) What kind of devices do you prefer to work with.
7) Do you store company files on your PDA?
8) How do Do you connect to the organization's data resources from your PDA?
9) Describe the security settings or configurations you have on your PDA.
10) Do you think antivirus should be used on a PDA? Explain.
11) Do you have a mechanism to wipe out data if you PDA is lost or stolen? Describe.
12) How do you know if your device has been compromised? Describe.
13) Policies followed by the company.
14) How well is your device protected.
15) Are you allowed to work from home with your device.
16) If so what are the security issues you face
17) Mobile apps used for working purpose
18) What recommendations can you make regarding the use of smartphones as working
19) Tools to make them more productive and less prone to risks
20) Risks faced by the company.
21) How is the company profited?

APPENDIX C

Duration

S.no	Candidates	Interview date	Mode	Duration
1.	Candidate 1	1 Nov 2014	In person	35 minutes
2.	Candidate 2	4 Nov 2014	In person	30 minutes
3.	Candidate 3	26 Oct 2014	Mail	20 minutes
4.	Candidate4	27 Oct 2014	Mail	20 minutes
5.	Candidate5	3 Nov 2014	Mail	20 minutes

BIOGRAPHY

NAME:	Ashwini Vasudevan
DATE OF BIRTH:	September 18th, 1991
EDUCATION:	
BACHELOR DEGREE	Bachelor of Computer Science(2013) R.M.K Engineering College, Chennai India
MASTER DEGREE	Master of Information Technology (2014) Stamford International University Bangkok, Thailand
NATIONALITY:	Indian
PRESENT ADDRESS:	6A, Regency Court, Soi 20 Sukumvit, Bangkok 10
EMAIL ID:	ashwini.v@stamford.edu
CONTACT NUMBER	(Thai)+66943313249, +917401131477(India)