A critical review of the governance of personal IT devices in work environments

Fatimah Alzair

A dissertation submitted to the Auckland University of Technology in partial fulfilment of the requirement for the degree of Master of Business (M.Bus.)

Faculty of Business, Economics & Law

2016

Primary Supervisor: Dr. Harminder Singh

Abstract

The purpose of this study was to review Bring Your Own Devices (BYOD) management practices by organizations. This study identifies the interests of employers and employees in a BYOD environment. The results of this study provide a useful reference for organizations implementing BYOD, as it provides guidance on how the process can be managed to achieve the goals of the organization. Theoretically, this study is going to contribute to research on information systems governance, in terms of understanding how the interests of policy makers and policy followers are balanced in practice and how this is reflected in the BYOD policy documents. This study was conducted using qualitative research design based on a thematic content analysis. This study utilises secondary data in the shape of electronic documents, corporate press releases, annual reports, and case studies on BYOD published between the years 2000 and 2015 entered into NVivo and the software helped in identifying various themes. The results of the study indicated that the issue of BYOD recently attracted the attention of researchers and practitioners as most of the research has been conducted from 2010 onwards. Moreover, the results also highlighted some themes like risks, challenges, benefits and organisational policy practices. Another finding about balancing the employees/employers interest has been discussed using agency theory and stewardship theory. The study also provides insight and guidance for future research in this area.

Table of Contents

Abstract i

List of Figures iv

Attention of Authorship v

Acknowledgements vi

Chapter 1: Introduction 1

1. Introduction **1**

1.1. Research Objectives 3

1.2. Research Questions 3

1.3. Problem Statement 3

1.4. Significance of Study 4

1.5. Structure of Thesis 4

Chapter 2: Literature Review 6

2.1. Chapter Overview 6

2.2. Mobile Devices 6

2.3. Usage of Mobile Devices 7

2.4. Threats associated with Mobile Devices 8

2.4.1. Major Sources of Mobile Threats **9**

2.4.2. Common Attacks on Mobile Devices **12**

2.5. Security of Mobile Devices 15

2.5.1. Types of Security Controls for Mobile Devices **16**

2.5.2. Security practices and weakness for Users of Mobile Devices **18**

2.5.3. Other Security Practices **21**

2.6. The "Bring Your Own Device" (BYOD) Phenomenon 22

2.6.1. Mobility **23**

2.6.2. Costs **24**

2.6.3. Security **26**

2.7. Theoretical Perspectives Underlying BYOD Policies 29

2.8. Conclusion 39

Chapter 3: Methodology 40

3.1. Chapter Overview 40

3.2. Research paradigm and Research Design 40

3.3. Population and Sampling 47

3.4. Data Collection 47

3.4.1. Journal Databases **47**

3.5. Data Analysis 50

3.6. Credibility of Research 53

3.6.1. Reliability of Study 53

3.6.2. Validity of Study 55

3.6. 3. Criticism of Data Sources 56

3.7. Conclusion 56

Chapter 4: Results 57

4.1. Introduction 57

4.2. Major Themes from the Data and how do they developed 57

4.3. Present Condition of BYOD Practices 58

4.4. Challenges caused by BYOD 62

4.5. Benefits of BYOD Practices 65

4.6. Organizational Policies for BYOD Practices 69

4.7. Conclusion 73

Chapter 5: Discussion and Conclusion 74

5.1. Discussion 74

5.2. Conclusion 78

5.3. Limitations of Study 80

5.4. Recommendations for Future Research 80

References 81

Appendices 87

Appendix 1: Results of Database Searches 87

Appendix 2: List of Studies Used for Review 88

List of Figures

FIGURE 1 HOW A BOTNET WORKS (SOURCE: BOTNET, N.D) 11
FIGURE 2: PHASES OF DATA COLLECTION... 50
FIGURE 3: WORD CLOUD QUERY 59
FIGURE 4: WORD TREE 61
FIGURE 5: MODEL FOR MAJOR RISKS... 63
FIGURE 6: TEXT SEARCH QUERY FOR RISKS 64
FIGURE 7: TEXT SEARCH QUERY FOR CHALLENGES 65
FIGURE 8: MODEL FOR BENEFITS OF BYOD.. 67
FIGURE 9: TEXT SEARCH QUERY FOR BENEFITS... 69
FIGURE 10: MODEL FOR DETERMINANTS OF BYOD POLICY 70
FIGURE 11: TEXT SEARCH QUERY FOR POLICY 72

Attention of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgments), nor material which to substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Fatimah Alzair

28 April, 2016

Acknowledgements

I am grateful to God for the good health and wellbeing that were necessary to complete this dissertation.

This dissertation would have not been a reality, if not for the wonderful people who supported, encouraged and most importantly, believed in me. To these individuals I offer my sincere and heartfelt gratitude.

Most importantly, I am extremely grateful to my Supervisor, Dr. Harminder Singh, for his excellent guidance in every aspect of this dissertation, from suggesting the topic till the end of this dissertation and for his patience and support which took me over numerous hurdles during this journey. He showered me with prompt, invaluable, detailed feedback on each chapter and encouraged me every step of the way.

I sincerely thank Annie McConnochie for all her efforts in proof-reading and editing this dissertation.

My great thanks and appreciation to my family especially my wonderful parents and my siblings in Saudi Arabia for their encouragement, prayers and best wishes despite the long distance from me. Without their love and support (especially my mother) I wouldn’t been able to accomplish this dissertation.

Finally, my warmest love and thanks to my lovely kids Besher and Roselle for their patience, support and understanding throughout my master study. I can’t express enough my feelings to my beloved husband Basil, who has been there for me from the beginning till the end of my Master Degree journey, every step of the way. Without your support, endless love and patience, I could not have reached for the stars. This journey has been filled with obstacles which have been challenging for both of us; however it is not the first, nor is it the last. I truly value the one thing that has remained solid over the many years of our relationship which is your enduring love, commitment, support, and for believing in me.

I dedicated this dissertation to my family especially to my lovely children Besher and Roselle and wishing them a very bright future.

Chapter 1: Introduction

1. Introduction

The concept of "bringing your own device" (BYOD) to one's workplace has recently emerged as an important issue for both practitioners and researchers globally. BYOD refers to the use of personal devices (such as smart phones and tablets) at work to access organizational resources such as email accounts, file servers, databases and other data, so that employers do not need to purchase and provide such devices to their employees (Calder, 2013). This trend has become common practice worldwide, with up to two-thirds of smart phones used in organizations being owned by employees (Armando, Costa, Verderame, and Merlo, 2014). By 2012, 95 percent of organizations in the United States allowed their employees to bring and use their personal devices for organizational purposes (Miller et al. (2012).

The practice of BYOD is gradually becoming popular in the business world today since it offers many advantages to both employers and employees. For example, if employees carry their own devices, such as laptops, smart phones or tablets to work, then they do not have to carry work-provided devices to work, significantly decreasing the burden on them. BYOD can increase productivity and innovation since employees are more comfortable using their own devices and organizations benefit from the latest capabilities on the devices, without having to find, buy and install them. Employees are also more satisfied when they use their own devices instead of devices issued by their firms (Miller, Voas, & Hurlburt, 2012)

However, it is not entirely clear whether allowing the employees to bring their own devices is the optimal choice for an organization. Allowing BYOD in an organization has implications for organizations and employees from many aspects, including extended mobility, IT costs, and security. There are many risks associated with the use of personal devices in the workplace. For example, the use of personal devices in workplaces has been accompanied by various security challenges for organizations around the globe (Miller et al., 2012). BYOD practices have also become the source of various types of cybercrimes; for example, hackers could obtain sensitive or private data or steal money and intellectual property by "hacking" employee-owned personal devices to commit fraud. Various BYOD governance policies and case studies have been written (Hunt, 2012), (Jindal, & Naik, 2013), (Scarfo, 2012), (Marshall, 2014) & (Freedman, 2012) to guide firms in managing the emerging trend of BYOD. The popularity of BYOD reflects a tension in employer-employee relations and has led to questions such as: should employees be encouraged to innovate and also to carry out their tasks? Should employers control what employees use to do their work? (Phillips, 2014)

This study will analyse the present state of BYOD management practices and policies in organisations. The upcoming sections of this study will extensively explore the related literature. BYOD management practices will be analysed through a qualitative study, in which content analysis is used to examine material related to BYOD from magazines, annual reports, policy reports, newspaper articles, journal articles and other sources. The major databases of published material include Wiley Interscience, Taylor & Francis, Sage Journals, SpringerLink, JSTOR, ScienceDirect, and Emerald Insight.

1.1. Research Objectives

The following are the objectives of this study:

1. To review the BYOD management practices and policies used by organizations
2. To assess the advantages and disadvantages of these BYOD practices
3. To assess the security threats associated with BYOD practices
4. To identify the interests of employers and employees in a BYOD environment, and examine how these are reflected in organizational BYOD management policies and practices
5. To suggest "best practice" guidelines for BYOD governance

1.2. Research Questions

This research aims to answer the following research questions:

1. How are the interests of employers and employees balanced in BYOD governance policies?
2. Why do organizations still allow BYOD use while there are many disadvantages and complexities associated with it?

1.3. Problem Statement

Researchers and practitioners involved in BYOD management practices speak about both the advantages and disadvantages of allowing employees to use their own devices at the workplace. BYOD practices favour both organizations and employees where complications can be reduced by having a strong device management policy. Despite the importance of the issue, little prior research has been conducted on it. It is also very difficult to find empirical studies on this issue as the field is at its early stages.

The major purpose of this study is to explore the current literature and review the recent material published in this field. Device management systems that are currently being used will be identified. In the end, the critical dimensions of a device management system will be discussed.

1.4. Significance of Study

From a practitioner's perspective, the results of this study provide a useful reference for organizations implementing BYOD, as it provides guidance on how the process can be managed to achieve the goals of the organization. Theoretically, this study is going to contribute to research on information systems governance, in terms of understanding how the interests of policy makers and policy followers are balanced in practice and how this is reflected in the BYOD policy documents. As IT becomes used even more frequently in individuals' personal lives, for example, with the use of smart-watches, it is necessary for organizations to have a better understanding of the impact of innovations on the governance of information systems. This study is one effort to that end.

1.5. Structure of Thesis

The entire study is divided into five chapters. First of all the introduction and background of the study is described in Chapter 1 which also includes the research questions, research objectives, research problem and significance of the study. Further Chapter 2 illustrates the past studies that have provided help in discovering the dimensions of the study along with determining the research questions and objectives of the study. Chapter 3 includes the methodology for the study and illustrates the approaches, data collection methods, research sample and sample size. In Chapter 4 the findings of the study are discussed which have been gathered through a qualitative study approach in terms of the analysis of the thematic content. The final chapter, Chapter 5, discusses and concludes the entire study and includes recommendations.

Chapter 2: Literature Review

2.1. Chapter Overview

In the first chapter, the background of the study was presented. Chapter 1 highlighted the research objectives, research questions, problem statement, and included an outline of the dissertation. In addition, the prevalence of technology in the business world, in general, and the "bring your own device" (BYOD) phenomenon, in particular, were discussed.

This chapter relates previous research on the BYOD phenomenon with the objectives and research questions of this study. It begins by providing some background information on mobile devices and their key vulnerabilities. Next, the chapter reviews the prior literature on the BYOD issue and summarises the perceived benefits, drawbacks, complexities, and problems caused by using personally-owned technological devices at work. Following that, two different philosophical approaches to managing BYOD are contrasted: agency theory and stewardship theory. The chapter concludes with some thoughts on the future of BYOD practices.

2.2. Mobile Devices

The BYOD phenomenon refers to the diffusion of personally-owned mobile devices into workplaces. The basic features of a mobile device, as listed in Scarfone and Souppaya (2012), were defined by the United States' National Institute of Standards and Technology (NIST). In short, a mobile device has the following characteristics: a small form factor, access to the Internet over a wireless network, and non-removable data storage. A mobile device utilises a full-fledged operating system, which is different from laptop or desktop operating systems, and various applications from third parties which are usually acquired over the Internet. Finally, such devices have the ability to synchronize their local data with remote locations, such as organizational servers, laptops, third-party servers, and the servers of telecommunications companies.

2.3. Usage of Mobile Devices

The usage of mobile devices in different forms and shapes is expanding at a rapid pace. In 2014, Cisco Systems forecasted that by the end of 2014, the number of mobile devices will exceed the number of people on Earth (CISCO, 2014). The historical data proved this forecast is true, as the number of mobile devices grew from 6.9 billion in 2013 to 7.4 billion mobile devices (CISCO, 2014). The Cisco report added that the trend of the number of devices being more than the number of inhabitants on Earth will remain in 2019, as the projected number of people will be about 7.6 billion in 2019. The Cisco report also predicted in 2014 that by 2019, the number of mobile devices per capita will be nearly 1.5. In 2014, the usage of smartphones increased tremendously as the growth rate was about 88% higher than the previous year (CISCO, 2014).

Innovations in mobile technology in the shape of third generation (3G) and fourth generation (4G) data communication standards have enabled mobile devices to acquire and transmit data much more quickly than before (Boyles, Smith, & Madden, 2012). The advancements in mobile devices have enabled users to obtain significant benefits, comparable to traditional laptops and computers. For example, you can now not only use mobile phones for calling others or for sending them text messages, but also for reading emails, storing notes, listening to music, playing games, watching movies, making video calls, staying connected with one’s family, friends and colleagues, and reading and editing documents on the go. Various software products for instance, social network applications like Facebook, WhatsApp, Telegram, and Twitter, as well as other basic applications like Note, Apple Music, and YouTube have enabled users to obtain such advantages.

At the same time, flaws in these software products may be exploited, increasing the vulnerabilities of individuals. These applications are also likely to cause some interruptions: since individuals are always trying to stay connected with their contacts, it becomes harder to ignore interruptions from these applications when carrying out other tasks. People are always on their phones receiving calls, checking out their friends on Facebook, chatting on WhatsApp, checking emails and listening to music. It has become virtually impossible to avoid unneeded interruption. It has also become difficult to avoid work-related emails and phone calls when you are at home with your family or on vacation (Ruggiero & Foote, 2011).

2.4. Threats associated with Mobile Devices

Some features of mobile devices place additional security concerns for organizations; for example, mobile devices usually have digital cameras, Global Positioning System (GPS) units, and microphones, support removable media, and can become removable media themselves by connecting them to USB ports (Scarfone & Souppaya, 2012). A mobile device can travel anywhere on the globe and connect to the infrastructure of its home organization once it returns, which poses considerable challenges for the security of data and sensitive information (Jansen & Scarfone, 2008).

These vulnerabilities have led to a rapid increase in the number of attacks on mobile devices in recent years. In 2012, the United States of America’s Government

Accountability Office reported that malicious threats for mobile devices in the shape of malware increased by 155 percent in 2011 alone, and the number of mobile device security vulnerabilities increased by 93%. In addition, the number of malware variants for mobile devices increased drastically and reached the figure of 40,000 (GAO, 2012).

2.4.1. Major Sources of Mobile Threats

The issue of cybercrime is faced by organizations globally. The term "cybercrime" is used to describe any illicit or illegal activity in which a particular network or computer is a target, tool or place used for any illegal activity (Taiple, 2012). Taiple (2012) adds that the major driving force behind any cybercrime is usually a financial gain. Cybercrime includes obtaining sensitive or private data through "hacking" (attacking IT systems to enter them without authorisation) techniques, so as to enable a person to commit a fraud. The theft of money, private data, and intellectual property are threats faced by commercial organizations and government agencies (GAO, 2012). Common motives for hacking sensitive information systems include harming national security, limiting the level of public trust in a government, hindering economic activity, and weakening and damaging vital infrastructure, such as electricity generation systems and mobile networks (GAO, 2012).

There are many sources of attacks on mobile devices, such as hackers, foreign governments, cybercriminals, botnet operators, terrorists, and national intelligence or counter-intelligence agencies (GAO, 2012). These entities are generally the owners of information systems which enable access to sensitive or private information resources through a malware code (Harris, 2010). For example, botnet operators compromise and control information systems for purposes such as transmitting attacks or illicit data on other information systems in return for a predetermined fee (Stallings et al., 2008). The word *bot* is a short form of “robot” and refers to computer systems that have been compromised and controlled by entities who do not own them (Stallings, Brown, Bauer, & Howard, 2008). “Botmasters” use the bots for masking the main source of information or data (Harris, 2010). Figure 1 shows how a botnet works; each of the steps is described in detail below (Gu, Zhang & Lee, 2008):

Step 1: Viruses or worms are sent out by a botnet operator to infect individual computers. The “payload” of these viruses or worms is a malicious application, the bot.

Step 2: Once the computer is infected, the bot logs into a particular command and control (C&C) server.

Step 3: The botnet operator sells access to the botnet to spammers.

Step 4: The spammers then send instructions to the infected PCs via the C&C server, so that they send out spam messages to mail servers.

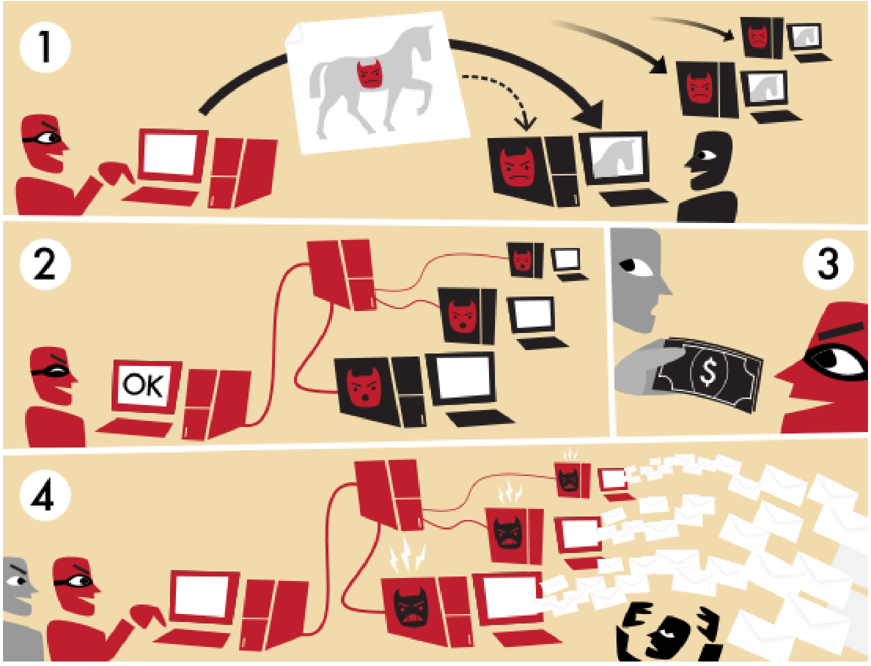

Figure 1 How a Botnet Works (Source: Botnet, n.d)

Another example of entities involved in attacking mobile devices are foreign intelligence services. At the data gathering stage, signals intelligence can be utilized by these services against mobile devices (ODNI, 2012). The development of solutions and tactics, techniques, and procedures (TTPs) to address such threats is usually supported by governments around the globe to disrupt or deny any illicit data approach, which is also vital to agencies such as defence and internal security (GAO, 2012). The information systems of U.S. companies and government agencies are targeted by more than 140 foreign agencies illicitly (Wilson, 2008).

It is important to mention that while hacking TTPs were difficult to acquire previously because they required deep knowledge of computers and programming, such skills can be easily and quickly learned nowadays; even novices can use downloadable scripts to hack computing systems, including mobile devices (Walker, 2012). This means that the number of potential sources of attacks has multiplied.

2.4.2. Common Attacks on Mobile Devices

The attacking entities discussed above can attack mobile devices by utilizing software, hardware, and users unlawfully. Examples of attack techniques include unauthorized location tracking, keystroke logging, data interception, spamming, network exploits, browser exploits, spoofing, phishing, zero day attacks, malware and loss or theft (GAO, 2012). These are described in detail below.

Keystroke logging is commonly used by hackers to obtain access to sensitive information such as credit card data, passwords, and banking information. Keystroke logging monitors the keystrokes on a particular target mobile device, and transmits the information gathered to a hacker's website or to an email address (GAO, 2012). A Trojan horse is often used to install "keyloggers" (Harris, 2010), especially because they cannot be detectable with typical security software (Walker, 2012). A Trojan horse is a programme that contains malicious or harmful code, and appears to be beneficial or harmless programming instructions or data, but can obtain control of a computer and damage it in many ways (Etsebeth, 2011).

Spamming is the process of sending unsolicited advertising and other commercial communications to a recipient. Spam can be sent via email or text messaging, which has become more frequent with the proliferation of mobile devices. This can create various problems for users, as they may have to incur additional costs by downloading unsolicited messages. Moreover, they have to manually delete every message or mail, which puts an extra burden on the user. Spam is also known to be an easy way of delivering malicious software (GAO, 2012).

The position of a mobile device can be identified through location tracking. Cybercriminals can track the location of a mobile device by using valid applications or by installing and configuring malware on the device. To use tracking legitimately, the consent and authorization of the owner of the mobile device is required, whereas this is not required if illegal means are used for tracking (GAO, 2012).

Another attacking technique is phishing, which has been discussed extensively in the literature. This is a type of social engineering with the sole purpose of gathering the financial data, credentials, personal information, and/or credit card information of an individual (Harris, 2010). Phishing can be done through pop-up messages attached to a particular website, or by emails from unknown sources, which successfully deceive mobile users to gain access to sensitive information. Various kinds of bait, such as notices that the recipient has won jackpots or lotteries, pornographic material, and promotions for instant financial gain (GAO, 2012), are employed by attackers to lure users and obtain the most sensitive information.

Hackers can also take advantage of weaknesses in software or web browsers, such as Internet Explorer, Firefox, and Chrome, to attack users. Through such browser exploits, malware can be installed without the knowledge of the mobile device's owner, and is usually done through associated hyperlinks and deceptive webpages (GAO, 2012). A new type of attack is data interception, and its purpose is to spy on data exchanges sent to or from a mobile device. There are various data interception techniques, with the most common one being the "man-in-the-middle" attack (MitM). When a user joins an unknown and unsecured Wi-Fi network, MitM enables a hacker to alter and capture the data packets on mobile devices. Public key certificates and digital signatures can reduce the chances of MitM attacks (Stallings et al., 2008). Sometimes, an attacker does not discard the data captured through the MitM attack but instead transfers it to another recipient on an unencrypted network (GAO, 2012).

The growing use of the Bluetooth data transfer technology in mobile device has led to new forms of attacks, such as Bluesnarfing and Bluejacking. Bluesnarfing refers to the act of unauthorized access from a wireless device for the purpose of gaining access to personal information, via a Bluetooth connection between laptops, desktop computers, phones, and other mobile devices. Bluesnarfing enables an attacker to access confidential information, such as personal emails, text messages, calendar, personal pictures, videos, and contact lists without the consent and knowledge of the targeted device's owner. Bluejacking is not as harmful as Bluesnarfing, as the attacker only transmits data to a targeted device. Both of these attacks are done through Bluetooth connections, in which the targeted device is paired with the attacker's without the owner's consent. Mobile phone manufacturers were aware of these threats early on and have already enhanced Bluetooth pairing, so that both of these threats are not present in current mobile phone models (Walker, 2012).

The most commonly cited definition of malware is from the National Institute of Standards and Technology's (NIST) Glossary of Key Information Security Terms. The NIST defines malware as a program that is installed in a system without the consent and knowledge of the system's owner for the purpose of compromising the integrity, availability, and confidentiality of victim's operating system, data, or applications (Jansen & Scarfone, 2008)**.** Malware includes malicious logic, codes, and applets, and can take different forms, such as Trojan horses, viruses, worms, adware, and spyware (Kissel, 2012). Sometimes, malware can be automatically and unknowingly downloaded into a system and then executed to perform a particular unauthorized function. Malware can create harm in different ways by performing various functions, such as initiating telephone calls, accessing device locations, downloading harmful applications automatically, recording information by automatically activating the mobile device’s camera or microphone, and giving complete access to the browsing history of the mobile device (GAO, 2012).

2.5. Security of Mobile Devices

Government organisations like the Department of Homeland Security (DHS), the Federal Communications Commission *(*FCC*)* and National Institute of Standards and Technology (NIST), have stated that all smartphones and other mobile devices on a network should be considered unsafe until and unless they are strictly controlled by an organization’s centrally controlled system. All the mobile devices inside an organization must be monitored continuously to ensure the safety of the sensitive data and services of the organization (GAO, 2012). When a mobile device is not controlled by an organization, an organization may face various risks related to data protection, ownership of the data and security, which can be eliminated by authentication and encryption measures (Miller et al., 2012). Jansen and Scarfone (2008) argue that the overall security of the whole system must be taken into consideration during the planning phase because it becomes very difficult to address this once a system has been put in place.

Mobile devices are now vulnerable to attacks from hackers to the same extent as traditional computers and laptops (Viega & Michael, 2010). Thus, the threats associated with mobile devices should be considered in overall organisational security plans, or else the whole security infrastructure (security of the assets, networks and systems) could suffer the consequences (Rose (2012). The mobility aspect of a mobile device poses more risk to the loss of sensitive information theft than traditional computers, which are usually located in a fixed position (Jansen & Scarfone, 2008).

The cost of security assessment for mobile devices is higher compared to traditional computers, increasing the difficulties of ensuring a secure working environment in an organization (Viega & Michael, 2010). Applications in Android-based mobile devices function across different components with the help of middleware. This middleware is the weak point that helps hackers breach the whole system to gain access to users' personal and sensitive information. Furthermore, many businesses around the globe are facing problems because of the complex systems in such devices (Liu, Moulic, & Shea, 2010). Although organizations can use mobile device management (MDM) software to manage individual mobile devices, this requires more effort, time, and cost. Using MDM may also lead to additional security concerns, as it is usually unable to manage the applications installed on individual devices (Miller et al. (2012). Moreover, the short length of passwords and weaker encryption standards also place considerable threats on the system (GAO, 2012). Despite these issues, proper MDM which "is the administrative area dealing with deploying, securing, monitoring, integrating and managing mobile devices, such as smartphones, tablets and laptops, in the workplace"(Le Grand , 2013) is not implemented in most organizations, as extra effort is required to ensure timely updates, patching and maintaining configuration standards which puts the whole system under the risk of various attacks (Scarfone & Souppaya, 2012).

2.5.1. Types of Security Controls for Mobile Devices

Various distinctive features of mobile devices, such as their small form and easy to hide structure, make these devices easier to be stolen than laptops and computers. Moreover, it is easier to retrieve a user's personal data from a mobile device than laptops and computers, which makes these devices more vulnerable. Under these circumstances, the implementation of additional security measures can ensure the efficient management of mobile devices over a network. An extensive review of published material in the area of mobile devices did not provide a consensus for any single software or program for combating all of the threats associated to mobile devices (Calder, 2013). Mobile users must be conscious enough to combat the attacks (Wilson, 2008). Meanwhile, the literature provided some key controls which can help in minimizing the chances of vicious attacks over mobile devices. In order to ensure the physical security of a mobile device, user authentication in the shape of a lockout password or pin could be useful (GAO, 2012).

Boyles et al. (2012) found in their research that over thirty three percent of mobile devices have usually been stolen or lost. These huge figures necessitate the need to have such a program installed in mobile devices which would enable users to remotely wipe sensitive and personal information from the devices remotely. This could help in saving the contents even after a mobile device has been stolen (GAO, 2012). Moreover, the installation of a whitelisting policy over a mobile device which would only allow certain specified applications to be installed on the device can also reduce the chance of any malware or spyware. The GAO (2012) stressed the importance of taking precautionary measures beforehand as this can add layers of security on a device. The author added that the probability of having the wrong combination of precautionary measures should also be reduced as it can create a hindrance to the efficient functioning of mobile device.

A centralized security management system in an organization will help it generate a holistic view of the condition and state of its mobile devices, and whether they are compliant with set rules and policies or not (GAO, 2012). Such systems should include management permission and configuration control, to permanently mitigate the chance of the presence of any malware in the entire system.

The growing equipment inventory puts an extra burden on organizations as they have become over-tasked (Liu et al., 2010). To safeguard the productivity of device management, proper implementation, tight enforcement, and continuous monitoring is very crucial (Liu et al., 2010). In today's business environment, continuous connectivity to the internet is vital for profitability, leading companies to ensure their employees have undisrupted connectivity by providing them with mobile devices (Schultz & Shpantzer, 2010). Under these circumstances, security professionals have a huge responsibility for the proper management, accountability, and protection of mobile devices, the same as they have for conventional computers (Microsoft, 2006). Some large companies such as Apple and Microsoft have also incorporated MDM features into their operating systems and architecture designs (Schultz & Shpantzer, 2010). Presently, there are also some companies in the market which offer MDM solutions for organizations.

GAO (2012) asserted the importance of having an enterprise firewall to prevent any unauthorized traffic to and from mobile devices connected to a network. Real-time status reports can also be gathered through automated software tools which could help in monitoring compliance with a set of rules and policies. Moreover, mitigation steps for any type of risk can also be carried out with the help of active and passive scanning of compromising events (GAO, 2012).

2.5.2. Security practices and weakness for Users of Mobile Devices

As the weakest link in most systems, users can minimize the threat of attacks by following some key security practices. Mobile device users often use public Wi-Fi networks, which are usually exposed to various security vulnerabilities (Miller et al., 2012). Singhal (2002) highlighted some of the major vulnerabilities in using public Wi-Fi networks. One of the major threats is that the hackers search for devices connected to public Wi-Fi networks whose default settings can be changed by a third party. Another threat is associated to peer-to-peer intrusion in which the attacker targets other clients over the same network. The broadcasting of internet traffic is also possible for nearby users over the same Wi-Fi network. Moreover, the attackers can also intercept and modify data sent to and by particular users on the same network. Attackers can also install malicious software products onto a particular device in a Wi-Fi network. If users minimize their exposure to public Wi-Fi, then they can reduce the chances of exploitation (GAO, 2012). User security is highly dependent upon mobile device settings, but most users are not familiar with this (Miller et al., 2012).

Moreover, software programs for mobile devices that are unsafe or unwanted should not be installed to avoid any potential security exploitation (GAO, 2012). Boyles et al. (2012) found that around thirty-eight percent of adults in the United States alone downloaded suspicious apps in 2011. The study also found that more than fifty percent of users had deleted at least one app from their mobile devices, which was used to gather too much personal information without the consent of the user.

Most of the apps available in app marketplaces usually collect the personal data of users from time to time and then pass or sell this information to third parties (GAO, 2012). A mobile apps industry survey has also acknowledged the fact that most of the apps utilize undefined and illicit ways of gathering information (GAO, 2012). Large firms in the IT industry, such as Hewlett-Packard, Google, Apple, and Amazon, have agreed to improve their privacy policies to avoid and mitigate the chances of illicit data collection procedures (Boyles et al., 2012). So, organisations need to be careful of what their employees install on their devices, because dodgy applications may steal confidential commercial or governmental information.

Miller et al. (2012) suggested that the least amount of personal information should be shared over the Internet. To mitigate the chances of data theft, it is necessary for users to take appropriate security measures when sharing personal information on the Internet when using their mobile devices. The chances of phishing can also be reduced by not sharing mobile numbers on public websites as the mobile could be attack when using the internet (GAO, 2012). The authors added that if the users put their devices in discoverable mode then the device becomes more vulnerable for attacks. This is all because the discoverable mode makes the device visible to others in the nearby area which makes it very easy for hackers to attack the device.

The chances of mobile device theft can be considerable reduced by implementing controls, such as authentication and authorization controls to prevent unauthorized access to mobile devices and the data on them. The sensitive information such as passwords, credit card information, and other monetary information must not be saved in a mobile device (Miller et al., 2012). The very well-known practice of “jailbreaking” should not be carried out, because it bypasses and limits operating system restrictions and integrated security settings of the devices, making them more vulnerable to attacks (Scarfone & Souppaya, 2012).

To ensure an efficient and risk-free working environment, continuous monitoring and enforcement of security policies for mobile devices is very important (Liu et al., 2010). Adherence to organizational policies, management, and control of mobile devices can be ensured through having a centralized security management system (Jansen & Scarfone, 2008). During the implementation of an enterprise mobility solution, it is very important to consider mobile device scalability and security to mitigate the risk associated with it like putting critical data on networks that are not secure (Liu et al., 2010). Mont and Brown (2011) argue that automated tools help in decreasing the risk of misconfiguration during IT provisioning which is "in charge of assessing the suitability of users to get user accounts and access rights and granting these access rights"(Mont & Brown, 2011, p.5) and deprovisioning which is "in charge of removing access rights and user accounts, when no longer needed by employees" (Mont & Brown, 2011, p.5). Both deprovisioning and provisioning are considered to be important for managing system access rights and user accounts. The chances of system exploitation, which would enable acts such as illicit access to sensitive information and misuse of credentials, increase considerably with any mistakes in the implementation process (Mont & Brown, 2011).

2.5.3. Other Security Practices

The vulnerabilities of attacks and threats can also be reduced on mobile devices by implementing some additional security practices which can help organizations considerably. The implementation of a uniform set of practices for the whole organization and policies to follow can also help in this regard (GAO, 2012). The overall awareness about the matter can also be increased by organising training sessions in the organizations. The timely identification of mobile threats, and for their appropriate elimination, organizations must ensure proactive measures (GAO, 2012). In order to achieve organizational IT security objectives, a well-thought and well-developed mobile deployment plan can help considerably (GAO, 2012). The authors also added that there must be a centralized mobile device configuration management system in an organization’s network infrastructure.

2.6. The “Bring Your Own Device” (BYOD) Phenomenon

The consumerization of IT has been largely stimulated by the increase of mobile device capabilities and its usage. One of the most cited definitions of IT consumerization is by Regard (2012, p. 10), who defined it as “the purchase of devices by employees who then petition IT to allow their integration into the corporate systems.” The usage of personal devices for work is also known as the “Bring Your Own Device” trend **(**BYOD) (Rose, 2012).

The main motivator for organizations to take advantage of the BYOD trend is to save costs (Miller et al., 2012). About eighty percent of adults in U.S. own mobile phones, out of which about forty five percent own smartphones (Miller et al., 2012). Users quickly become attached to their own mobile devices, which makes it very difficult for them to switch to other corporate-provided devices as a routine (Armando et al., 2014). While some organizations restrict the use of personal devices in organizational premises and do not allow personal devices to connect to organizational networks (Rose, 2012), many other organizations are allowing the use of personal devices for organizational purposes, mainly because doing so lowers their costs while extending the mobility of their employees (Schultz & Shpantzer, 2010). Miller et al. (2012) found that 95 percent of organizations in the U.S. allowed their employees to bring and use their personal devices for organizational purposes. The next section discusses the organisational and individual consequences of allowing BYOD use in organisations.

2.6.1. Mobility

The term mobility in the BYOD context refers to a characteristic of the employee which is not limited by a fixed location or an office (Miller et al., 2012). A study of IT directors in the U.S. found that employee morale improved with the introduction of a mobile-centric workplace (Miller et al., 2012). The authors also found that it brought out the positive attitude of employees and increased the level of employee retention. Loose, Gewald, and Weeger (2013) found that the device an employee chooses in their private life is superior to that which a company may provide, so they prefer to use their own devices for both organizational and personal purposes. The study also found that employees are more willing to use their personal device based on the idea that it reflected flexibility, mobility, and the characteristics that would create job longevity. According to their study, the company's face value to an individual had a positive correlation with the intent to use a personal device at the workplace (Loose et al., 2013). Loose et al. (2013) asserted that the implementation of BYOD has significantly improved employees' productivity, mobility enhancement, and helped in ensuring a more flexible work environment.

Ortbach, Köffer, Bode, and Niehaves (2013) found that the ease of use of the technology matters to most people in the choice of IT device and mobility contributes a lot in terms of the ease of use of communication devices. While working with a personal device, employees can basically work everywhere, and whenever they like. Lebek, Degirmenci, and Breitner (2013) argued that organizations are willing to implement mobile devices into their IT infrastructure to take advantage of the level of flexibility these devices offer. An efficient implementation of BYOD policy encourages employees to innovate without any restriction. Consumerization on an individual level is of interest in various research studies in this area as Dernbecher, Beck, and Weber (2013) found that self-efficacy and personal innovativeness can considerably be increased by using private technologies for official tasks (Dernbecher et al., 2013).

Mobility through BYOD in organization might have positive and negative influences. Dernbecher et al. (2013) found that employees appreciate flexible working procedures, which leads to heavier workloads for people working in the company. Niehaves, Köffer, Ortbach, and Katschewitz (2012) found that through IT consumerization managers are more likely to give employees work tasks during off-hours keeping in view the extended level of mobility of employees. This leads to longer hours, which can result in extra fatigue for employees (Niehaves et al., 2012). At the same time, it brings many benefits for employees as mobility due to BYOD provides more flexibility. The freedom of choice regarding work contributes to the happiness of knowledge workers (Niehaves et al., 2012). If an organization adopts an open workplace policy that allows employees to get their work done from wherever they want to do it, the organization must also identify their management needs regarding network security (Niehaves et al., 2012). A first step towards reaching this goal is to gather all concerned stakeholders to revise the existing policies. Mobility is thus an important factor to positively influence workers to use BYOD. Another significantly important factor for companies to consider is the cost factor.

2.6.2. Costs

It is necessary to consider a variety of costs while assessing BYOD implementation. The costs of BYOD use are less important in monetary terms, while the cost of losing important and sensitive information is more severe. Calder (2013) argued that mobile devices are like a Pandora’s Box, filled with personal and corporate data free for a criminal once he or she has access to the data. Rose (2012) found that the usage of a mobile device lends itself to further threats since there is no total control over the device which can create serious problems for organizations. If an employee with strong customer relations or clients leaves the company for another, the cost could be disastrous (Rose, 2012). According to Loose et al. (2013) there are two perceived threats to a business that allows personal devices to be used at the workplace: i) a decline in performance, and ii) privacy breaches (Loose et al., 2013).

Despite these issues, BYOD may still lead to positive outcomes for an organization. It increases employee satisfaction and accelerates the use of the newest technology within the organization (Calder, 2013). The type of company and the willingness to implement BYOD in the workspace is also significant. Niehaves et al. (2012) found a difference in the willingness to implement the use of BYOD in the public and private sectors due to costs. The public sector often has a low IT budget and a sensitive image they convey to citizens, because all financial expenses are drawn from taxes that are collected. When employees fund their own devices, BYOD may have even more positive effects for their organizations, as employees make a capital investment that benefit their organization and reduces the costs of IT in organizations, since organizations just have to pay the operational fees and the need to make investments in purchasing the devices is eliminated (Niehaves et al., 2012). However, there is still a big “but” in the investigations into BYOD. This has to do with security. Even though allowing BYOD may be good for organizations by increasing employees’ satisfaction and mobility, and reducing other costs, what about security for both companies and employers?

2.6.3. Security

Although some of the points associated with security are also discussed in Section 2.4, these concerns require further explanation. Rose (2012) found that one of the major problems in regard to BYOD usage is the potential for confidential data to be at risk through privately-owned devices. Miller et al. (2012) noted that an added security risk would come if employees lose their phones with company data on the devices (2014). The author also found that about 60% of the companies have not yet taken any type of security measures for securing organizational data. Niehaves et al. (2012) also found in their study that about 75% of IT managers are significantly concerned regarding the security of BYOD. Miller et al. (2012) suggested the organizations consider taking severe actions in regard to managing and monitoring instant messaging, video and photography storage, email and texting, internet browsing, device tracking, and even “wiping” the device clean, even though the devices are personally owned. Miller et al. (2012) suggested that a company must secure corporate information through passwords or even dual verification authentication and there must not be a choice when it comes to the implementation of a security measure. Ortbach et al. (2013) found that IT consumerization behaviour is strongly connected to data security and violation policies which means that the tighter the data security policies are, then there would be a positive impact in terms of IT consumerization. According to Ortbach et al. (2013) colleagues, direct superiors, and friends are the most influential normative referents affecting the IT consumerization intention.

Employees generally agree with the implementation of BYOD because of the perceived benefits. However, they often are unaware of their responsibilities for the security of corporate information assets (Lebek et al., 2013). This causes a problem, because it might mean that employees do not use BYOD as they should, i.e. by following corporate security policies for mobile devices. This increases the risk of their employer losing much of the benefits that they would obtain if BYOD is being properly used.

A solution could be the use of mobile device management (MDM) technology, which enables firms to enforce security policies on devices owned by employees (Lebek et al., 2013). However, MDM may limit the devices' functionality and firms may find it difficult to enforce its usage on privately-owned devices compared to corporate assets (Lebek et al. 2013). It is possible that employees would feel secure about operating in a BYOD environment if MDM was deployed, and that the benefits of IT consumerization would manifest themselves in organisations.

Calder (2013) provided suggestions for organizations on how to protect and to regulate the personal use of a privately-owned device that is being used as corporate device, filled with sensitive data. These are:

a) keeping a record of the International Mobile Equipment Identity (IMEI) number,
b) installing a password, and
c) Mandating encryption on mobile devices and for corporate email to protect personally identifiable information.

Armando et al. (2014) writes about an approach to securing BYOD in companies based on the concept of a secure meta-market (SMM), which mediates access to traditional application markets, keeps track of the apps installed in registered devices, and checks whether new apps respect a given organization's security policy. A secure meta-market guarantees that a set of applications installed on a mobile device comply with a given security policy (Armando et al., 2014). The work of Armando et al. (2014) shows that extending the mobile application distribution model is feasible to provide security for BYOD in organizations by means of a secure meta-market in combination with a given security policy (Armando et al., 2014). This is important, because it means that any organization will be able to make use of such a secure meta-market in order to protect itself and its employees.

The three major stakeholders of BYOD practices are owners, employees and management, and they all have concerns with the prevalence of BYOD at the workplace. Olalere, Abdullah, Mahmod, and Abdullah (2015) argued that BYOD enables employees to be more mobile and gives them flexibility to choose the best device as per their work requirements. The authors also found that BYOD increases the productivity of employees. Meanwhile, management also enjoys various benefits from BYOD as it gives easy access to its employees anywhere, anytime, and also saves a tremendous amount of costs in purchasing the devices for employees from the corporate budget (Mahesh & Hooter, 2013). Some of the major benefits of BYOD include cost savings, employee flexibility, management flexibility, simplified IT infrastructure, and increased employee contentment.

There are also some concerns shared by all the stakeholders. While the employees want to have convenience, at the same time they also require a certain level of privacy in terms of their personal information on their device (AirWatch, 2012). Along with this, the biggest challenge for management is the transfer of corporate information on the devices that are not managed by the IT department. There are strong chances of data theft, leakage, and a failure to comply with regulations (Morrow, 2012). Nevertheless, Morrow (2012) associated with that the challenges associated to BYOD that do not undermine the importance of BYOD for both employees and management. Morrow (2012) further added that management understands the importance of BYOD and usually tries to find solutions for ensuring data security.

The preceding sections have summarised the benefits, costs and potential risks of adopting BYOD in workplaces. Organisations that allow or support BYOD use in their workplaces have put in various policies and guidelines to manage the trade-offs between the possible positive and negative outcomes of BYOD use. These organisational policies are a reflection of the relationship between the owners, managers and staff of the organisation. The next section discusses two theoretical perspectives on this relationship and explores how they are related to the use of BYOD.

2.7. Theoretical Perspectives Underlying BYOD Policies

Two theories that can be used to understand BYOD and its practical implications are agency theory and stewardship theory. This section will discuss the implications of both of these theories as they relate to the issue of BYOD.

Between agency and stewardship theory, the former is the dominant theory in organisational research in many ways (Donaldson & Davis, 1991). Agency theory focuses on the nature of the relationships and the dynamics between the principals and agents within an enterprise/business (Shapiro, 2005). Inherent to agency theory is the idea that although it is presumed that company employees, employers, and shareholders share the goal of doing what is best for a company, their intentions can manifest themselves in different ways, and may lead to conflicts (Jensen & Smith, 2000). In turn, such conflicts must be addressed and, more importantly, remedied as expeditiously and competently as possible in order to prevent further issues and escalate problems that can hurt an organisation's bottom line (Jensen & Smith, 2000).

Underlying agency theory is the idea that individuals, especially those operating in Western-culture oriented enterprises, are driven to a large degree by ego and the desire to pursue their ambitions through their organisation. This can sometimes be construed as anti-social and undermine the overall ability of a company to ensure trust and camaraderie, something that may be more easily attained in Eastern-culture oriented enterprises, such as those in Confucian cultures (Ardichvili et al., 2012; Jensen & Smith, 2000). Whilst this does not automatically mean that employees cannot do right by their employers, and the shareholders of the companies for which they work, this perspective complicates the scenario. This is especially the case when the issue of BYOD arises, something to be discussed herein.

In contrast to agency theory, stewardship theory offers an alternative explanation of the way in which various actors operate within firms. It presupposes that, even in Western-culture oriented enterprises, although individuals may certainly exhibit ego-centric traits and seek to pursue their professional goals at the workplace, which is a reasonable expectation for many professionals, that is not the paramount driver of their behaviour (Hernandez, 2012). Rather, employees, along with their supervisors, collaborate far more frequently and successfully than not; they act as truly social creatures rather than anti-social beings who are out only for themselves (Donaldson & Davis, 1991; Fox & Hamilton, 1994; Hernandez, 2012).

Stewardship theory provides a stark contrast to the dystopian firm environment proffered by agency theory. This is because it makes space not so much for the possibility that employees and managers typically work together, but rather because it puts forth the narrative that this is not just a possibility, but a regularly occurring reality, especially because constant conflicts are too costly to be sustained indefinitely (Hernandez, 2012). Thus, equilibrium is found through cooperation, something that occurs in many facets of a company's culture.

However, with the influx of personal electronic devices, gaps have been created in which such collaboration has been undermined by issues revolving around communications and trust concerning the use of personal devices in the workplace. This has been the case especially since many employees feel that they should be entrusted to maintain their devices and even those of employers, whereas employers feel that their need to safeguard information should be respected, a legitimate claim concerning the preservation of proprietary information. By being able to significantly scrutinise what employees do with such devices in the workplace, employers have increasingly sought to implement BYOD policies that are mutually beneficial. However, companies have failed precisely because they fail to integrate an understanding of the theoretical implications of such policies on the organisational psychological well-being of employees as a pro-social unit (Hernandez, 2012).

Per an agency theory evaluation of the issue, the problem is quite clear: employees and employers are inherently divergent in their needs and pursuits. Although both parties seek to increase their access to funds – for the former, it is for wages or a salary and for the latter, it is for profits – there is a lack of synergy. The result is uncertain, since the overall foundation of the relationship is not based on mutual trust, understanding, or reciprocity of aid, good faith and good will, but is instead a zero-sum game (Gavetti, 2012).

In contrast, following a stewardship theory evaluation of the issue, the problem is a bit more nuanced, fluid, and arguably allows for mutually beneficial remedies. Under this approach, managers or supervisors look out for the best interests of their shareholders and thus the overall bottom line of an enterprise by behaving such that their actions align with the best interests of the employees they are overseeing (Davis, Schoorman, & Donaldson, 1997). There is a horizontal rather than a vertical hierarchy of considerations and knowledge sharing that increases the health of the organisation by seeking to cater to, within reason, employees' requirements (Boussebaa, Sturdy, & Morgan, 2014; Goyder, 2011).

The underlying assumption of the stewardship theory is that all parties working for any given organisation share the broad understanding that everyone works to increase the chances of organisational survival and improvement (Goyder, 2011). This can only be achieved when there is harmony and parsimony within an organisation, which demands the help, motivation, and goodwill of employees (Vallejo, 2009). As such, with respect to BYOD policies, a stewardship approach, in contrast to an agency approach, would be predicated on creating internal governance mechanisms in which the rights of employees and employers are both protected, and those rights are accompanied by responsibilities and duties that have to be upheld by both parties for everyone's mutual benefit (Davis et al., 1997).

Whilst both agency theory and stewardship theory focus on problem-solving and the nature of professional relationships, the former is more oriented towards problem-solving while accounting for presumed anti-social or undermining behaviour, and the latter focuses more on relationships, expecting individuals to increase their social productivity to innovate and move beyond temporary problems. Thus, whereas agency theory addresses the prevention of losses due to divergent principal and agent goals, stewardship theory examines the pursuit of innovation and consensus which can be used to solve problems. Energy is thus expended differently with each approach, and companies whose managers' philosophies belong to either of these backgrounds will be likely to address company issues concerning BYOD, in particular, in a similar fashion. This can help or hinder progress in how employees and employers balance the rights of each party in the workplace.

In general, both agency and stewardship theories maintain that equilibrium between employees and employers or perhaps more appropriately, employees and managers/supervisors, can be achieved and maintained under certain circumstances. In particular, this typically involves ensuring that both parties act to increase their own independent and interdependent utility (Corbetta & Salvato, 2004). Moreover, in order to protect shareholder interests, keep agency costs in check, and establish interest alignment between agent and principal, agency theorists have suggested multitudinous governance instruments (Bertoncini, Griesert, & Magette, 2012). However, while this approach can be optimal for companies in a BYOD policy context, its bias towards companies, sometimes at the expense of employees, can undermine both company viability and employee well-being, both of which ultimately influence company survival. Instead, per (Davis et al., 1997), different approaches, often left up to the discretion of individual companies, are needed to protect the rights of both parties in a manner that is mutually beneficial (Corbetta & Salvato, 2004).

The lack of existing literature on BYOD policies indicates that to best understand how to adequately address the issue, specifically with respect to balancing the rights of employees and employers, the boundaries of each party must be identified, as well as the areas in which there is divergence and convergence of interests. For employers, there is the inherent need to assume responsibility for a number of areas related to business operations to effectively protect their enterprises from potentially catastrophic obstacles, such as those capable of leading to firm failure. These are logistical issues and include the assumption of risk for "legal, security, reputational, and other business-related risks when their employees use a device for both personal and work-related purposes" (Bertoncini et al., 2012, p.2). These issues are relevant since a company must be able to control its workplace environment to ensure it operates in a legal and ethical manner and survives.

In terms of communications and intelligence-sharing, the issue becomes that much more relevant because, increasingly, employees have the means to help companies they work for and also hinder them and sabotage them for any number of reasons via the unauthorized dissemination of mobile devices, sometimes which are more portable and advanced than those owned by the employer (Thomson, 2012). The unauthorized dissemination of information by mobile devices can lead to a chaotic atmosphere in which employees can realistically begin to have a level of de facto power compared to employers, causing a threat to operations and thus disturbing the aforementioned equilibrium (Thomson, 2012). As a result, companies require the ability to act, essentially, as benevolent dictators – to maintain control, while allowing for a certain amount of employee flexibility so as not to starve employee comfort, innovation, and ultimately, employees' sense of belonging at an organisation, something which is foundational to their ability to positively impact the organisation for which they work (Aycan, Schyns, Sun, Felfe, & Saher, 2013). This could be achieved in a manner that bridges agency and stewardship approaches if done with great foresight and an evaluation of the behavioural issues at play with firm cultures (Wiseman, Cuevas-Rodríguez, & Gomez-Mejia, 2012).

When employees are permitted to bring their own devices to work, to use for both work and personal endeavours, employers lose control and employees gain control. This has been noted. However, this does not necessarily have to be a zero-sum game, depending upon how policies are set up (Hernandez, 2012). In order to return to or maintain equilibrium, there must be mechanisms by which both parties have ground rules which, if broken, lead to real consequences (Chiva & Habib, 2015; Nord, 1969). Such consequences are essentially a means of conditioning or modifying behaviour, either after an infraction has occurred but, more proactively, over time, to prevent the majority of infractions from occurring (Chiva & Habib, 2015). The nature and scope of consequences must vary based on the type of infraction, which often relates to the type of information that may be improperly revealed, for example, proprietary, health, legal, or financial. Improper disclosure could be a matter of unintentional or intentional actions and must therefore be dealt with, via an effective BYOD policy, accordingly.

Each type of information is associated with different types of improper disclosure problems. Per the literature, it is important to note, however, that behavioural techniques aimed at conditioning employees, in particular, to handle company information cautiously, are a matter of organisational psychology as much as anything else, namely business administration (Chiva & Habib, 2015). From a psychological perspective, for employees to do their due diligence to follow BYOD policies, especially as these policies are typically established solely by their employers rather than collaboratively with employees, they must realistically have some belief that the policies are socially acceptable and beneficial (Al-Omari, El-Gayar, & Deokar, 2012). Regardless of whether such policies are actually legal and make sound business sense, the ultimate test for employees before they accept these policies, as least with regard to management and organisational psychology theory literature, is whether or employees feel slighted by such policies, have their rights and freedoms (perceived or otherwise) unduly constrained, or whether they are appreciative of the reasons for such policies (Al-Omari et al., 2012).

Additionally, the way such policies are received by employees may also be affected by the manner in which they are conveyed. That is, have they verbally been communicated to employees, individually or within a group, or were they conveyed via written documents, such as employee handbooks or an employment contract (Hu, Dinev, Hart, & Cooke, 2012)? Employee affect (that is, their response or resultant emotion) towards a BYOD policy is affected by, among other factors, how the information is conveyed and how employers create an environment that seems safe for employees to bring up potential grievances, questions, or issues with said policies (Hu et al., 2012).

The situation, however, concerns the interests of employees, as well as the interests of employers and how those are framed and, more importantly, conveyed. As smartphones and other personal electronics become ubiquitous, employees using these devices can pose several problems for employers looking to strike a balance – an equilibrium – between keeping their employees happy, and also allowing company business to proceed as needed. For example, employees may be more comfortable with the configuration and design of their own devices, while employers may be wary of data "leaking" from employees' devices if they install malicious apps that siphon data away secretly.

Personal electronic devices can especially pose a problem for employers with regard to privacy (Barnes, 2013). Though they are personal devices, employers can address privacy matters through a well-thought-out "bring your own device," or

BYOD policy, focused on shared interests and shared space (Barnes, 2013). Employers may choose to eliminate expectations of privacy on both company and personal devices that are used for business, or they may choose to allow a certain amount of privacy for employee's own personal use, with the employer still retaining the right to monitor or access the device (Barnes, 2013; Hinkes, 2013).

The determination as to which should be pursued must likely derive from the type of organisation a company is, its organisational philosophy and culture, and ultimately, the types of information the company finds it necessary to shield (Hinkes, 2013). In such types of BYOD policies, an employee may have an expectation of privacy, except in previously-determined and agreed upon situations, such as in the event of a termination or litigation. In keeping with what is known about agency as well as stewardship theories, such a hypothetical limited expectation of privacy, though tempered, could very well be acceptable because it is framed and conveyed in a mutually beneficial and socially understandable and acceptable manner (Barnes, 2013; Hernandez, 2012; Hinkes, 2013).

Moreover, employers realise that issues can arise if the security of devices is compromised, as in the instances of a theft or hacking, and the security of sensitive company information can thus also be compromised. A well-crafted BYOD, at least in theory, *must* allow for the retention of all company data and trade secrets. Employees can be entrusted with data, in a tiered manner so as to condition employees regarding how to act appropriately with such information, which protects a company as well as its employees, likely shielding both from various types of fallout. In instances in which personal and private information are both contained on an employee's personal device, the compromised security of the said device can mean that the employer's information is also compromised, and that the employer would need to pursue actions in order to keep the information secure, such as wiping data from the device. It is therefore in the employee’s own interest, to have a back-up of all photos, contacts, and other personal information contained on the device, and also to proactively ensure that such personal information passes strict scrutiny with regard to appropriateness. In short, each party – employee and employer – must continuously be on their best behaviour.

Despite the privacy and security concerns, the usage of employee-owned devices for job-related business has its benefits for both the employer and the employee. For instance, due to lease agreements and other such obligations, employer-issued devices such as smart phones, tablets, and laptops may be older, and generations behind the current technology, something mentioned in the beginning of this section (Barnes, 2013). This can result in a less-than-efficient use of company time, and therefore ultimately costs the company money. Employee-owned devices are often newer and, therefore, more user-friendly and efficient (Barnes, 2013). Additionally, a BYOD policy allows employees to have only one device to worry about, instead of being responsible for both personal and professional devices. This is a technological example as well as an extension of the synergy that stewardship theory presupposes occurs between employees and employers in the activities of a typical firm (Gavetti, 2012).

Ultimately, many companies have already adopted and embraced a BYOD policy, or are planning to do so (Hinkes, 2013). Although the privacy and security concerns are very real and, in some cases, pronounced, a BYOD policy also allows employees to use newer technology (therefore being more efficient with their time) and eliminate the use of multiple devices which represents (pro)socially positive effects for the companies for which said employees work (Belle, 2015). A well-crafted and properly-implemented BYOD policy strikes a balance between the employer's and employees' needs—employer security with employees' right to privacy, resulting in increased accessibility and overall higher morale and workplace satisfaction.

2.8. Conclusion

This chapter helped in understanding the issue of BYOD, its present condition, organisational policies, and advancements in published research articles. Moreover, the threats, attacks, and vulnerabilities associated with mobile devices are also discussed. There is no doubt in the fact that allowing employees to bring their own devices at the workplace has benefits for both employees and employers. Even so, at the same time, there are some associated issues with BYOD which organisations as well as employees have recently been faced with. Keeping in mind the complexities generated by BYOD, the management of companies still want to gain the benefits of the BYOD phenomenon, because this brings greater value to all of the stakeholders. The next chapter discusses the methodological aspects of this study.

Chapter 3: Methodology

3.1. Chapter Overview

The previous chapters have presented the background of the study, its objectives, the research questions, and an overview of the relevant literature. This chapter describes the methodological aspects of the study, namely the research design, population, sampling frame, data collection methods, and data analysis techniques. In addition, the various tools used to collect data from different sources are also discussed in this chapter. This chapter is organized as follows:

i. Research Pardigm and Research design;

ii. Instruments used for collecting data;

iii. Methods of analysis used to address the research questions, and ensure the credibility and validity of the results.

As a reminder, this study's research questions are:

1. How are the interests of employers and employees balanced in BYOD governance policies?
2. Why do organizations still allow BYOD use while there are many disadvantages and complexities associated with it?

3.2. Research Paradigm and Research Design

Research paradigms address the philosophical dimensions of social sciences. A research paradigm is a set of fundamental assumptions and beliefs as to how the world is perceived which then serves as a thinking framework that guides the behavior of the researcher (Jonker & Pennink, 2010). Although the philosophical backgrounds usually remain implicit in most research, they affect the practice of research. Some writers (e.g. Berry & Otley, 2004; Creswell, 2013; Saunders, Lewis and Thornhill, 2009; Neuman, 2011) emphasizes that it is important to initially question the research paradigm to be applied in conducting research because it substantially influences how one undertake a social study from the way of framing and understanding social phenomena. Following this suggestion, various research paradigms are discussed below to enable a justification of the theoretical assumptions and fundamental beliefs underpinning a social research.

Positivist researchers seek to obtain law-like generalisations, termed nomothetic research (Neuman, 2011), by conducting value-free research to measure social phenomena. Positivists believe that different researchers observing the same factual problem will generate a similar result by carefully using statistical tests and applying a similar research process in investigating a large sample (Creswell 2013). Their common belief is the existence of a universal generalization that can be applied across contexts, which is now called naïve realism.

Postpositivists challenge the belief of this absolute truth, especially in relation to studying human behavior in social science. The postpositivist approach also believes in generalization, but admits that knowledge is a result of social conditioning. This is called the critical realist stance, which means that understanding social reality needs to be framed in a certain context of relevant law or dynamic social structures, which have created the observable phenomena within social world. Interpretivism, at the far extreme of postpositivism, subscribes to what is called constructivism.

Interpretivists believe that reality is constructed by social actors and people’s perceptions of it. They recognize that individuals with their own varied backgrounds, assumptions and experiences contribute to the on-going construction of reality existing in their broader social context through social interaction. Because these human perspectives and experiences are subjective, social reality may change and can have multiple perspectives (Hennink, Hutter & Bailey, 2011). Therefore, interpretivists reject objectivism and a single truth as proposed in postpositivsm. To understand the social world from the experiences and subjective meanings that people attach to it, interpetivist researchers favor to interact and to have a dialogue with the studied participants. They also prefer to work with qualitative data, which provides rich descriptions of social constructs.

As opposed to the generalization or nomonethic approaches adopted by postpositivist researchers, interpretivists use a narrative form of analysis to describe specifics and highly detailed accounts of a particular social reality being studied, which is termed the idiographic approach (Neuman, 2011). Consequently, the parameter to test knowledge in the positivist and interpretivist paradigm-camps is distinct. Positivist scholars believe in the power of replication research. Interpretivist researchers regards a study that uncovers inside perspectives or real meanings of social phenomena from its study participants as good social knowledge.

In terms of axiology, intrepretivist researchers take the themic stance or the insider perspective, which means to study social reality from the perspective of the people involved themselves. Here, the experiences and values of both research participants and researchers substantially influence the collection of data and its analysis.

This objective of this study is to review organisational BYOD management policies and understand the interests of employers and employees and how they are taken into account in the policies. In keeping with this objective and the study’s research questions, the study utilises qualitative research techniques. For the purpose of analysing the data, thematic content analysis was used. Qualitative research is a naturalistic approach (Lincoln & Guba, 1985), which helps in understanding the true meaning of people’s decisions, beliefs, actions, feelings, and values associated with a particular issue or as a whole in their social lives (Ritchie & Lewis, 2003). A qualitative research approach also helps in elaborating how people interpret and make sense about the world around them (Zimmerman & Szenberg, 2000). Furthermore, qualitative research constitutes a rich description of places, people, experiences, and conversations which formulates the social reality (Denzin & Lincoln, 2004).

One of the major characteristics of the qualitative research approach is its enormous flexibility which allows researchers to have access to important and unexpected findings, which cannot be discovered through pre-determined questionnaires (Smith & Osborn, 2003). Qualitative research techniques enable researchers to have a holistic and comprehensive view of the social setting in which a particular study is conducted. Along with this, various researchers have asserted that social life is actually a series of events and each event must be analysed so that the reality of an individual’s daily life could be explained in a better way (Seale, 1999). Qualitative research techniques analyse and describe the behaviours of individuals, cultures, and social groups in reference to the subject matter (Berg, 2007). While commonly used for primary data, the qualitative approach is also equally appropriate for analysing secondary data such as governmental reports, articles, case studies, advertisements, and newspapers (Seale, 1999).

The qualitative research approach is a non-statistical methodological approach which is guided by concrete material (Berg, 2007). It is important to mention that in the quantitative approach, the main focus is to use the data with the help of statistics and show the data in tabulation form. The findings of any quantitative study are usually descriptive in nature and the numerical framework is the centre of its conclusions (Bogdan & Biklen, 1992). While it is widely assumed that a qualitative study is subjective and a quantitative study is objective, various researchers regard this as an oversimplification (Bogdan & Biklen, 1992). The authors argued that qualitative and quantitative studies differ in that qualitative research is usually a more in-depth exploration of a subject area, whereas quantitative studies are usually focused on explanations. In recent times, quantitative research studies are seen as having the goal of developing universal laws, whereas qualitative studies emphasise the exploration of dynamic, emergent realities (Berg, 2007). The major differences between qualitative and quantitative research studies are as follows:

- Qualitative research methods use documents, focus groups, and in-depth interviews whereas quantitative studies use experiments, structured interviews, structured observations, surveys, and numeric information in documents and records.
- Induction is primarily used in qualitative studies, whereas deduction is used in quantitative studies to develop hypotheses from existing theory and pre-specified constructs.
- A common perception is that qualitative studies are more subjective in nature, since the problems and conditions are described from the point of view of those who are actually experiencing it, and that quantitative studies are more objective, since they rely on more well-defined constructs. However, as previously mentioned, this tension can be considered an oversimplification, as it ignores the subjectivity inherent in quantitative research, in terms of, for example, the selection of the sample, the data

cleaning methodology, the choice of analytical techniques, and the way the research problem is perceived in the first place (e.g. cross-sectional vs. longitudinal, single vs. multi-level, mono vs. cross-cultural).

- Qualitative studies contain more in-depth information whereas while quantitative studies are less in-depth at the same time they have a greater breadth of information about various cases.
- Qualitative research studies present semi-structured or unstructured response options to respondents whereas quantitative studies present fixed response options.
- Whilst the reliability and validity of qualitative research studies is dependent upon the skills and expertise of researcher, the validity and reliability of quantitative studies is based upon the instrument used or the data measurement device. Both can be equally risky.
- More time and resources are consumed during the analysis phases of qualitative studies whereas in quantitative studies, more time and resources are spent during the planning phase.

It will not be wrong to say that qualitative studies have rich and detailed data whereas quantitative studies generate generalizable data and findings which are deduced from the cause-and-effect relationships of the dependent and independent variables (Ritchie & Lewis, 2003). Another benefit of conducting qualitative studies is that fewer resources are usually required (Denzin & Lincoln, 2004). The authors highlighted that the number of respondents in qualitative studies can be between 5 and 20, depending upon the nature of the study, whereas the minimum number of respondents required to have sound results in quantitative studies is about 200.

Moreover, the respondents of qualitative studies are given more liberty in order to express their views about a particular problem or situation.

Keeping in view all of these differences between qualitative and quantitative studies, this study uses a qualitative approach. The focus of this study is to examine the principles underlying the BYOD policies and practices used in organizations around the world, not the impact of these policies on people or employees. The study is based on examining the organisational response to BYOD. For this, previously published material was gathered and analysed by utilizing the qualitative approach. This was accomplished by keeping in mind the various benefits associated with this approach. At first, the nature of the study demanded utilizing the qualitative approach. Secondly, the main purpose behind conducting this study was to have a detailed analysis of this issue according to the organizations, and the researchers. Furthermore, the qualitative approach gives a deeper understanding of the issue to be researched (Denzin & Lincoln, 2004). On the other hand, in the situation where resources both in regard to time and money are limited, then the qualitative approach is the best solution. Keeping in view all of these benefits, the qualitative approach is the most suitable for this study.

Qualitative data can be collected through various ways such as sustained contact with respondents or informants or by analysis of available materials such as magazines, annual reports, policies, newspaper articles, and any sort of information published about a particular subject (Bogdan & Biklen, 1992). Moreover, qualitative research enters the world of the people who are to be studied and keeps all of the records for what s/he hears and observes during the whole process of study (Bryman, 2001). With the purpose of finding the common elements in BYOD governance policies, and the balance of interests of both employers and employees in BYOD governance policies, a qualitative research design was deemed to be most appropriate for this study, especially since it has been used in related research such as (Vandelannoitte, 2015).

3.3. Population and Sampling

The population in this case is the academic and practitioner literature on BYOD management, and the sample is the particular set of observations that were gathered based on the study's criteria. This study utilises secondary data in the shape of electronic documents, corporate press releases, annual reports, and case studies on BYOD published between the years 2000 and 2015. The emergence of handheld devices and portable personal computers including laptops started from early 2000 and along with this, the issue of BYOD also emerged.

3.4. Data Collection

For a clear understanding of the issue of BYOD and gathering all of the published materials, reports, and case studies related to this area of research, various sources were utilized during the data collection process. In order to find and gather as much relevant information about the subject area as possible, library search engines and online sources were used which helped considerably to have a more comprehensive literature study and to gain a better understanding of the research problems.

3.4.1. Journal Databases

Auckland University of Technology's library has access to major sources of published materials such as Wiley Interscience, Taylor & Francis, Sage Journals, SpringerLink, JSTOR, Science Direct, and Emerald Insight. These databases contain published materials such as electronic journals, books, and case studies which helped considerably in accessing most of the information related to this area of research. After getting access to all of the related information and published data, the screening process started for the literature found from the online libraries. These search terms were used: "*bring your own devices at workplace*", *"organization policies for BYOD"*, *"advantages of BYOD policy"*, *"issues related to BYOD policies"*, *"impact of BYOD on employee satisfaction and performance"*, *"case study of BYOD"*, and *"cost related issues to BYOD"*. Appendix 1 (Results of Database Searches) lists the number of documents that were found for each search term within each database.

Another resource, Google Scholar, was also used to find related material to this area. In the last few years, the introduction of Google Scholar has been very helpful for scholars around the globe for finding the relevant literature for a particular research study. Google Scholar is a search tool which looks similar to the main Google search engine and focuses on scholarly sources, such as journal articles, research papers, conference papers, theses, books, reprints, abstracts, case studies, and technical reports from many areas of study, ranging from social sciences to engineering, psychology, law, public administration, management sciences, and many more. During the search of data related to BYOD, keywords such as *"bring your own devices at workplace"*, *"organization policies for BYOD", "advantages of BYOD policy"*, *"issues related to BYOD policies"*, *"impact of BYOD on employee satisfaction and performance"*, *"case study of BYOD"*, and *"cost related issues to BYOD"* were put in Google Scholar search interface.

In total, 250 published documents, consisting of articles, chapters, and case studies were found, and among these 60 most related published articles and case studies were found to be the most appropriate for this study. During the screening process, only 40 were regarded as primary sources (listed in Appendix 2: List of Studies Used for Review) and the rest were either excluded or rejected. The screening process was conducted manually by checking the amount of space devoted to the issue of BYOD in each document. The articles, reports, and case studies which have the highest number of words written on the issue of BYOD were selected for further analysis. These 40 articles and case studies were separated according to their relevance to the topic. Along with this, some of the documents were also obtained through examining electronic sources such as Lexis-Nexis and ProQuest, as well as corporate press releases, annual reports, and vendor case studies.

Figure 2 shows the phases of data collection by screening the inappropriate materials. It is also important here to mention that Google Scholar was used to assist in finding the research reports, articles, and case studies. The main function of Google Scholar during data collection was to reach the source of data. For example, if a term is searched in Google Scholar, it shows the links of articles in a particular library or electronic database. Moreover, Figure 2 also shows the number of articles and reports which were collected and screened in each step, and the number of papers and reports used to answer each research question. Once they were identified, their conceptual and theoretical models were summarized. Next, the narratives of each document in each research tradition were mapped by using citation-tracking software and manual searches of electronic databases. Within each stream, the key elements, the key actors, the organisations, individuals and industry associations, were identified and events in its development, and the metaphors used by its proponents to describe it.

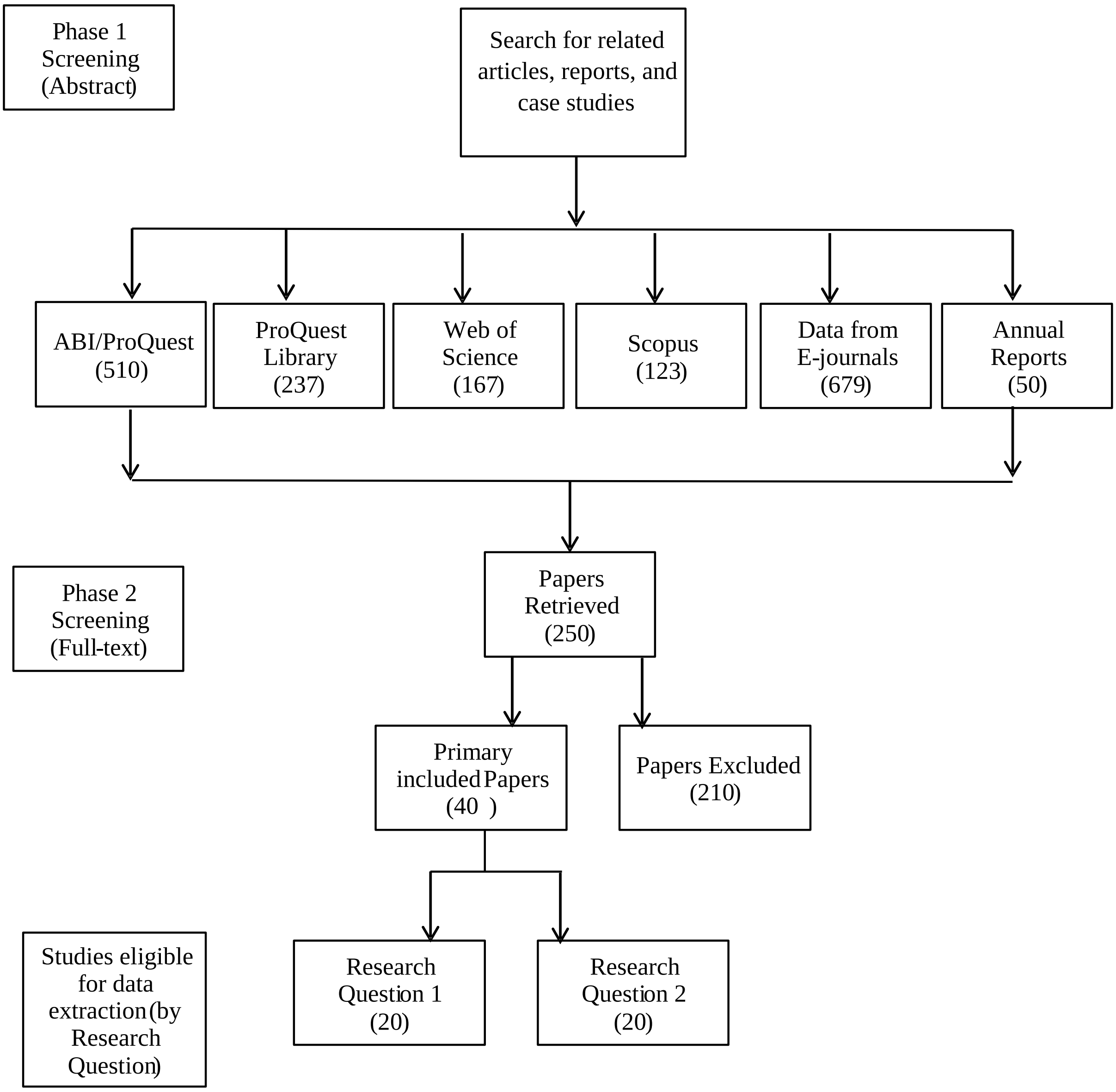
Phase 1 Screening (Abstract)
Search for related articles, reports, and case studies
ABI/ProQuest (510)
ProQuest Library (237)
Web of Science (167)
Scopus (123)
Data from E-journals (679)
Annual Reports (50)
Phase 2 Screening (Full-text)
Papers Retrieved (250)
Primary included Papers (40)
Papers Excluded (210)
Studies eligible for data extraction (by Research Question)
Research Question 1 (20)
Research Question 2 (20)

Figure 2: Phases of Data Collection

3.5. Data Analysis

For the purpose of analysing the data, thematic analysis (Braun & Clarke, 2006) was used. It is also known as category-based-analysis (Weber, 1990) or theme-centred analysis (Schorn, 2000). Researchers have argued about the benefits of thematic analysis, such as its enablement of theoretical freedom (Braun & Clarke, 2006). The two types of thematic analysis that can be found include theory-driven thematic analysis and inductive thematic analysis (Frith & Gleeson, 2004). While the coding and themes are linked to data themselves, then this sort of approach is known as inductive approach (Patton, 1990). The author added that inductive thematic analysis is closely related to grounded theory. In inductive thematic analysis, since there is no pre-existing coding frame, it can be said that this approach is data-driven. Through this approach, a detailed analysis of various aspects of data can be made possible (Patton, 1990).

In contrast to this, theory-driven thematic analysis is derived by the researcher's analytical and theoretical interest in a particular area of research (Frith & Gleeson, 2004). The choice between the theoretical and the inductive approach is largely dependent upon the coding and organizing the various themes with respect to the data (Patton, 1990). The data analysis which is conducted in this research thesis is driven both by the nature of the data and theoretical interest so this analysis is considered an inductive content analysis. Since this research study is targeted towards finding the relationship between the theoretical perspective about the subject area and the data, it is considered inductive analysis.

At the start, I began the data analysis process by reading all of the literature available from various sources such as magazines, annual reports, policies, newspaper articles, and any sort of information published about a particular subject from the online databases mentioned previously. As mentioned all of the related information has been screened according to its relevance to the topic. Furthermore, in the second reading of both the related information in annual reports that outlined BYOD policies and the journal articles, I performed line by line coding of the information which ascribed each sentence in the data. The initial coding of this study was based on my own theoretical understanding about this area of research. The coding method or the codes themselves were based on the data as per the suggestion recommended in the previous literature (Braun & Clarke, 2006). The further steps of data analysis constitute the merging of all the codes in to larger units which are also based on the information gathered. This process of merging the codes into larger units was continued until only a few codes remained.

The next step constitutes the generation of themes which integrated the codes into certain themes. Various practitioners and researchers highlighted the importance of the themes generation process and regarded it as the most crucial phase of thematic content analysis (Braun & Clarke, 2006). In regard to creating themes from the codes it was difficult as it is nowhere mentioned from the sources of data or any specified guidebook about the generation of themes or what formulates a pattern. For the purpose of analysing the collected data, this study regarded themes as the smallest unit which would be able to express the codes in a meaningful way that were created in the previous step. For example, an underlying concept can be represented by a theme based on the codes that gives true or near-to-real expression of codes. At the end of this step, five themes were generated from various codes and described what is generally written about BYOD in articles, research papers, conference papers, theses, books, reprints, abstracts, case studies, and technical reports.

Usually, thematic content analysis has been critiqued for losing the overall picture of a phenomenon, because the codes are commonly separated from the original context. It is also said that thematic content analysis is usually a more person-centred approach of qualitative data analysis (Braun & Clarke, 2006). Nevertheless, from an extensive review of the literature for the purpose of determining the most appropriate analysis technique, thematic content analysis is the most suitable technique for this study. A well-known qualitative data analysis software, NVivo, was used during the data analysis. Version 10 of NVivo was utilised for the analysis. All of the data gathered was entered into this software and the codes and themes were formulated in this software. In recent times, NVivo has proved to be an essential tool for information management and measurement for qualitative studies. Various analysis queries were applied in NVivo such as cloud tags, word frequency, text searching, and word tree.

3.6. Credibility of Research

Ensuring the credibility of any research study particularly for a qualitative study is very crucial and there are some predefined measures which must be taken by a researcher. The concepts of reliability and validity were explained by Creswell and Miller (2000) and Seale (1999). The trustworthiness of a study is extremely important and for this a research study must be in accordance to two previous studies and the methods of a study must also be in accordance to previous studies. Not only this, the previous studies must be from the same area of research. Therefore as the researcher, I undertook some measures to ensure the credibility of this study and also to avoid the occurrence of any inaccuracy which are as follows:

3.6.1. Reliability of Study

In order to enhance the reliability of this research study, the code creation and theme generation processes were undertaken by two persons separately and then the common codes out of each person’s assessment were considered. In terms of the measurement regarding the extent to which the raters or the data collectors assign the similar scores for a particular variable, this process is known as interrater reliability (Patton, 1990). There are various ways to analyse interrater reliability, and in this study, I use the most common method, Cohen's Kappa. The value of Kappa ranges from -1 to 1. The value of Kappa is derived from the following formula:

$$\kappa = \frac{P_A - P_c}{1 - P_c}$$

Where:

P_A= proportion of units on which the raters agree

P_C = the proportion of units for which agreement is expected by chance.

The benchmark for Kappa value is suggested by Landis and Koch (1977) which can be seen in table 3.1.

Table 3.1. Benchmark for Interpreting Kappa Value

Kappa Statistics	Strength of Agreement
<0.00	Poor
0.00 – 0.20	Slight
0.21 – 0.40	Fair
0.41 – 0.60	Moderate
0.61 – 0.80	Substantial
0.81 – 1.00	Almost Perfect

The value of the Kappa statistic for this study was 0.79 which is regarded as highly substantial. Previous research found a higher risk of errors when only one person coded documents, and researchers are thus advised to use at least two persons for the assessment (Berg, 2007). This approach was very useful for reducing coding errors. The same approach was carried out for the theme generation process.

3.6.2. Validity of Study

To enhance the authenticity and also to increase the validity of findings, the measures suggested by Johnson and Christensen (2004) were considered for this research. As per their research, researcher bias, theoretical validity and descriptive validity were considered for this study. The use of two raters helped in reducing the researcher's bias whereas the theoretical validity was ensured through an extensive review of literature.

Second, researchers have also suggested to obtain an expert's opinion from a person who has previously done similar work in the same area. For this, a researcher named Rachel Thomson was contacted by mail. She is the Director of the Centre for Innovation and Research in Childhood and Youth, at the University of Sussex. She worked previously with the London South Bank University, Open University, and University of Manchester. She is a sociologist by discipline. Her research interests are in the interdisciplinary fields of sexuality and gender studies. Ms. Thomson was kind enough to share her thoughts about the topic and the research technique incorporated in this study. I gave Ms. Thomson an overview of my study and she replied giving me with following suggestion:

"Hello, after going through the overview of your study, I suggest you stick with the qualitative approach for your study as the topic is newly emerged and there is not much written on this topic. So, I suggest you go through most of the related material and analyse the material through NVivo. Moreover, I also suggest that you work on the reliability and credibility of the research as this is the major concern of any qualitative study. Meanwhile, I think that you must do the coding of the data with at least two interpreters because this will increase the reliability of study. I also suggest that you apply the queries such as cloud tags, word frequency, text searching,

and word tree in NVivo. That's all I suggest to you for your research. I wish you best of luck for your study."

3.6. 3. Criticism of Data Sources

The major critique about the data sources used in this research study is its reliance exclusively on secondary data. This study did not collect any primary data, which means that no interviews or surveys were conducted with employees, managers, or practitioners. Secondary data was used because of a scarcity of resources and time limitations, as well as the objective of the study, which has been to examine the state of the field. Future researchers in this area should use primary data if they have the time and resources so that they can capture the experiences of the individuals who use and manage such technologies in organizations. The results of this study will provide a clearly-defined base for further research in the future.

3.7. Conclusion

In terms of the data, this chapter has elaborated the tools and methods that have been applied. Moreover, the chapter also explains the overall design of the research. Meanwhile, the sources of data collection, such as, electronic journals, library search engines, and company reports are also justified. The chapter summarized that secondary data that is utilised during this research. Furthermore, the data is going to be analysed with the NVivo software, which is often used for qualitative data analysis.

Chapter 4: Results

4.1. Introduction

This chapter discusses the findings of the study that have been generated with the help of NVivo. As discussed in the previous chapter on the methodology, this study uses documents from various sources, such as magazines, annual reports, policies, newspaper articles, and other reports published about a particular subject from a wide range of electronic databases. All of the related material was then screened and in the end, 40 of the most appropriate articles, case studies, and reports were entered into NVivo for data analysis. Various descriptive and analytical methods were used in NVivo, such as cloud tags, word frequency, text searching, and word trees. This chapter starts with a discussion of the various themes that were found from the related material with the help of NVivo.

4.2. Major Themes from the Data and how do they developed

This study relied on thematic content analysis of secondary data. These themes were drawn by analysing the 40 articles, case studies, and reports, which were entered into NVivo. The software helped identify various themes such as the present condition of BYOD practices in organizations, issues related to BYOD practices, challenges caused by BYOD, the benefits of BYOD, security concerns, organizational policies for BYOD, and employee reactions to BYOD. Furthermore, the litreture review helped in the development of the themes. All of these themes will be discussed in the upcoming chapter, as well as how they help answer the research questions and fulfil the objectives of this study.

4.3. Present Condition of BYOD Practices

The comprehensive content analysis of the data presents the present condition of BYOD practices in various organizations around the world. BYOD is known to bring various benefits for the organizations and the most important benefit is the cost efficiency. Cost efficiency in a way that the organizations do not have to spend extra resources on providing devices such as mobile phones, and laptops, if employees bring their own devices and use these devices for personal and organizational benefits.

Still, it is also important to mention that the rise of BYOD has been accompanied by various issues, risks, threats and challenges for the organizations. Organisations are well aware of the benefits of BYOD so rather than prohibiting the use of personal devices at work, organizations are creating various policies to ensure an environment that is risk free. While it is undoubtedly true that the policy making for BYOD practices still require effort, the companies are taking some serious steps towards creating an environment that will be beneficial for both employees and organizations.

To better understand the present condition of BYOD practices and organizational responses, a word frequency query was run on the data. The results of word frequency queries are shown as word clouds and tree maps. Both of these techniques present deeper insights about the related material. Figure 3 shows the result of word frequency query in the shape of a word cloud. The figure shows that the most frequent words in the data were BYOD, devices, information, technology, employees, and so forth. Deeper observation of the word cloud query elaborates that the issue of BYOD recently attracted the attention of researchers and practitioners as most of the research has been conducted from 2010 onwards. This shows that the issue of BYOD requires much more effort to resolve the complexities caused by BYOD practices. The word cloud query also highlights the risks and threats associated to BYOD practices such as security threats, privacy issues, social issues, and technological complexities.

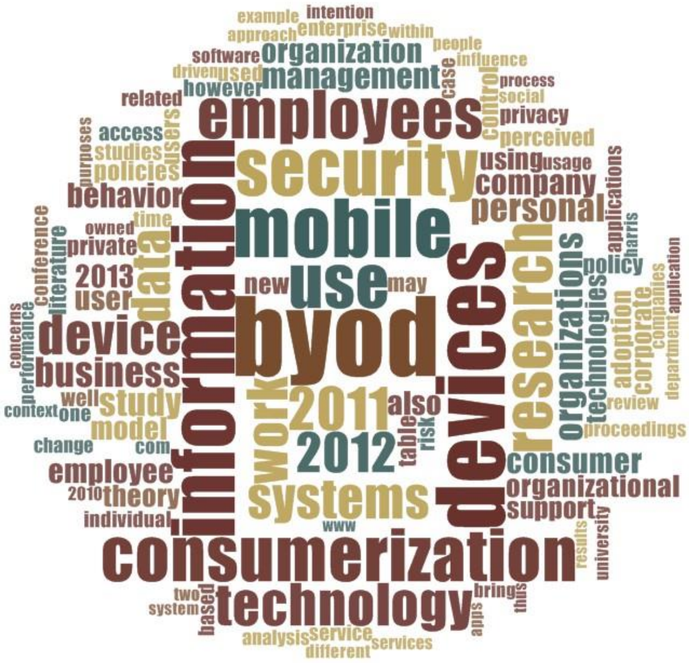

Figure 3: Word Cloud Query

The second shape of word frequency query is “Tree Map”. The Tree Map for the sampled data is shown in Figure 4. This diagram serves the purpose of showing the hierarchical data in the shape of various rectangles in different sizes. The size of the rectangles depends upon the number of coding references. A large rectangle is for the node that has a large number of coding references. In order to fit in all of the available space, the tree map is scaled accordingly. Meanwhile, the size of each rectangle in a tree map is usually considered according to the others. The tree map of sampled data shows that the terms such as BYOD, devices, mobiles, security problems, technological complexities, research, organizational policy, employees, and data issue have a higher number of coding references. This figure also illustrates that the years of 2010 onwards are counted as the time period in which the issue of BYOD gained the attention of researchers. This figure also highlighted the fact that the issue of BYOD practices is not only related to management, but also influences the fields of engineering and IT.

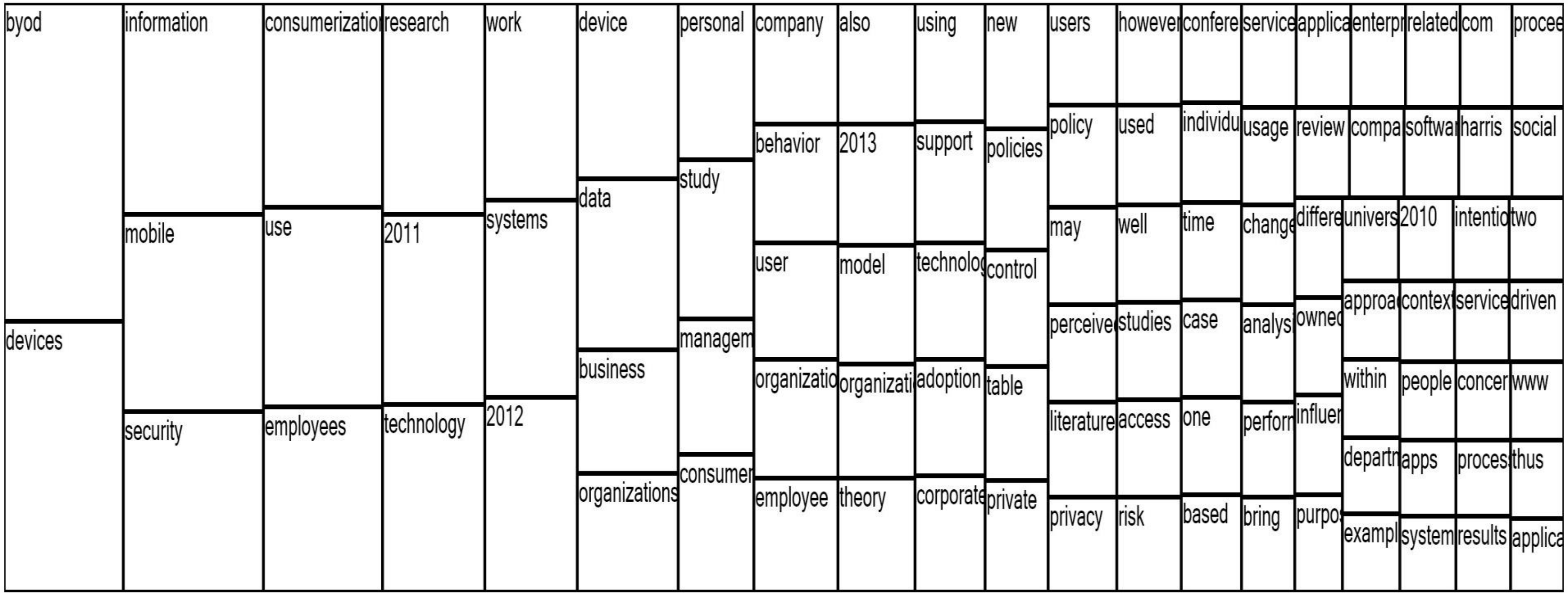

Figure 4: Word Tree

4.4. Challenges caused by BYOD

The deeper analysis of the sampled studies and data highlighted the fact that the introduction of smart phones and devices such as iPads, iPhones, Android-based phones and devices not only affects consumer behaviour it also affect the organizational working environment. The qualitative data analysis also highlighted that fact that employees are now adopting various unsanctioned devices at the workplace and this has placed different threats on corporate resources and raised various challenges for organizations around the globe. The value of using personal devices for management can be observed in recent times as the management of the companies stressed that the IT department should allow the use of these devices in order to have easy access towards required corporate information. This shift of business behaviour has created a number of challenges for IT companies since they do not have sole control over sensitive information and end-user tools as they previously had.

The second most important theme found from the sampled data through NVivo is the various challenges associated with BYOD practices. The software pointed out the challenges by various closely related nodes such as issues, threats, risks, and concerns. Moreover, there are many other risks that are highlighted during data analysis.

If the organization wishes to have efficient BYOD deployment at workplace then it is very important to have better insight of some of the major risks during policy development for BYOD practices. These risks are highlighted by Figure 5. This figure is actually an automatically driven model by assessing the nodes and coding.

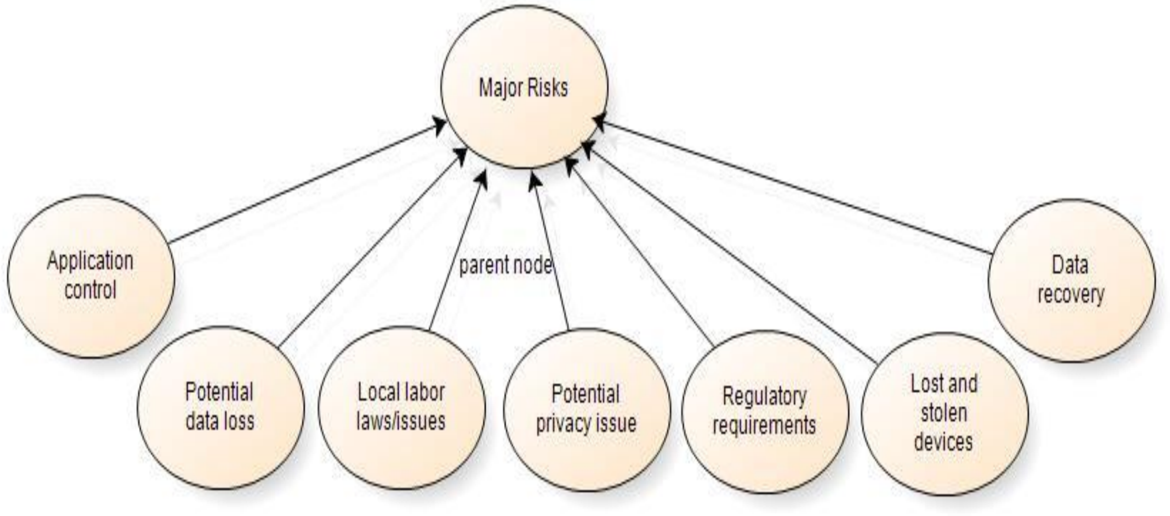

Figure 5: Model for Major Risks

By assessing the exported data the software automatically detected various risks associated to BYOD deployment. In this model, "Major risks" is the parent node and here are seven child nodes. The first risk is related to the unsecured and uncontrolled applications that are usually installed on end-user devices. The control of these applications is one of the major challenges for the organizations. The second risk is in terms of the potential data loss. Reducing and eliminating the chances of critical/sensitive data exposure is also a crucial challenge for organizations. Another challenge in BYOD deployment is related to local labour laws as various countries prevent the employees/users from working late and more than the specified working hours. In this case, organizations cannot ask their employees to work on their personal devices after the normal working hours although this is thought to be a normal practice in case of BYOD.

In order to have a better understanding, text search query was applied on sampled data with the terms such as risks, threats, and challenges. This helps in highlighting the major issues discussed in the data previously. Figure 6 shows the "text search query" with the searched term of "Risks". The figure pointed out various other threats such as the threat of malware, security implications and threats, threats for personal devices, threat of mobile phones theft, and many more. Figure 6 also highlights some real life examples of companies that are currently facing BYOD challenges such as IBM.

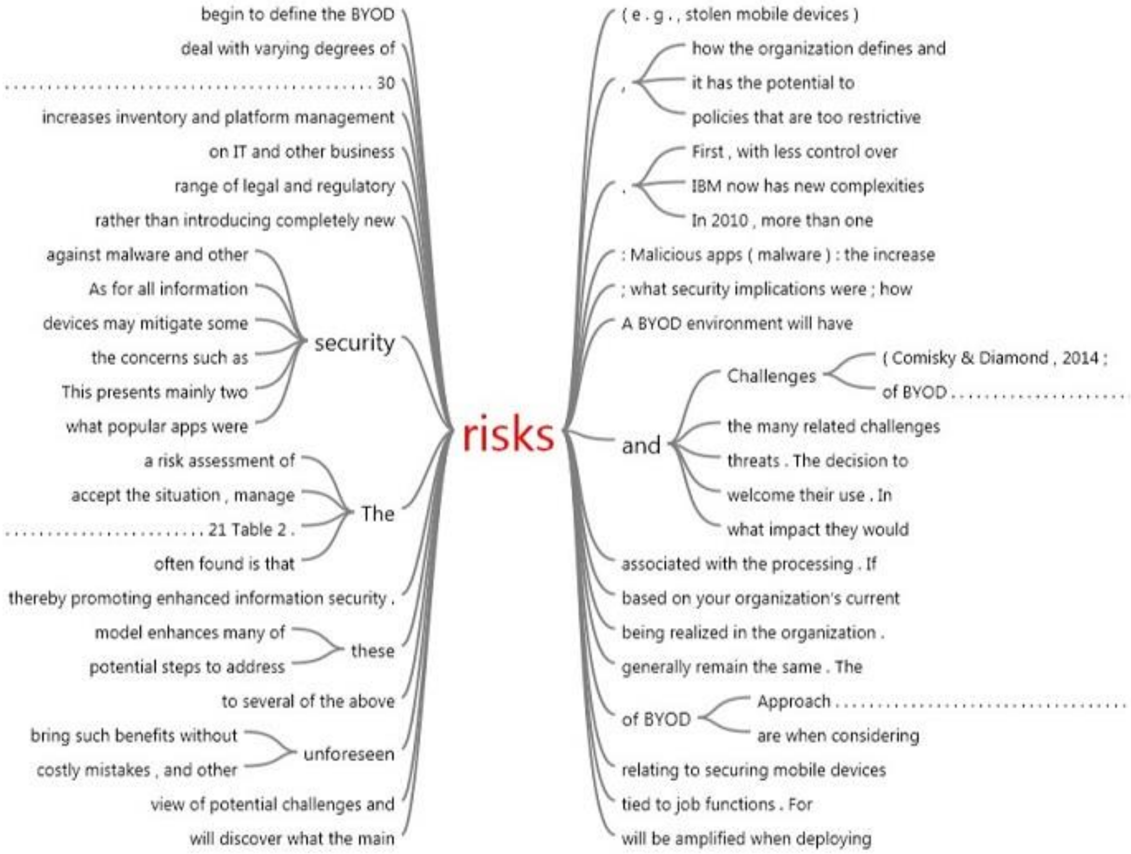
begin to define the BYOD
deal with varying degrees of
.... 30
increases inventory and platform management
on IT and other business
range of legal and regulatory
rather than introducing completely new
against malware and other
As for all information
devices may mitigate some
the concerns such as
This presents mainly two
what popular apps were
security
a risk assessment of
accept the situation , manage
.... 21 Table 2 .
often found is that
The
thereby promoting enhanced information security .
model enhances many of
potential steps to address
these
to several of the above
bring such benefits without
costly mistakes , and other
unforeseen
view of potential challenges and
will discover what the main
risks
(e . g . , stolen mobile devices)
,
how the organization defines and
it has the potential to
policies that are too restrictive
.
First , with less control over
IBM now has new complexities
In 2010 , more than one
: Malicious apps (malware) : the increase
; what security implications were ; how
A BYOD environment will have
and
Challenges
(Comisky & Diamond , 2014 ;
of BYOD ....
the many related challenges
threats . The decision to
welcome their use . In
what impact they would
associated with the processing . If
based on your organization's current
being realized in the organization .
generally remain the same . The
of BYOD
Approach ....
are when considering
relating to securing mobile devices
tied to job functions . For
will be amplified when deploying

Figure 6: Text Search Query for Risks

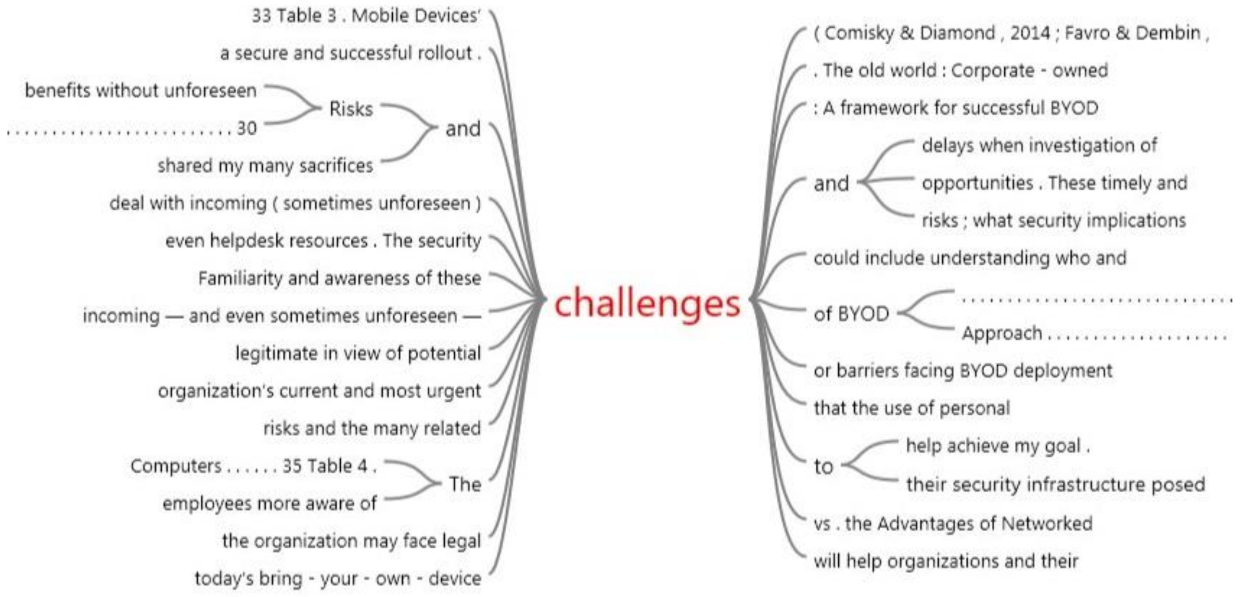
33 Table 3 . Mobile Devices'
a secure and successful rollout .
benefits without unforeseen
. . . . 30
Risks
and
shared my many sacrifices
deal with incoming (sometimes unforeseen)
even helpdesk resources . The security
Familiarity and awareness of these
incoming — and even sometimes unforeseen —
legitimate in view of potential
organization's current and most urgent
risks and the many related
Computers . . . . . . 35 Table 4 .
employees more aware of
The
the organization may face legal
today's bring - your - own - device
challenges
(Comisky & Diamond , 2014 ; Favro & Dembin ,
. The old world : Corporate - owned
: A framework for successful BYOD
and
delays when investigation of
opportunities . These timely and
risks ; what security implications
could include understanding who and
of BYOD
. . . .
Approach . . . .
or barriers facing BYOD deployment
that the use of personal
to
help achieve my goal .
their security infrastructure posed
vs . the Advantages of Networked
will help organizations and their

Figure 7: Text Search Query for Challenges

Another "text search query" was applied to the sampled data with the name of "Challenges". This brought up with the results shown in Figure 7.

4.5. Benefits of BYOD Practices

The previous sections of this chapter discussed various challenges faced by organizations with the presence of BYOD practices. There is no doubt in the fact that along with the challenges faced by organizations during BYOD deployment, there are also various benefits associated to the use of BYOD practices. The data analysis identified the different benefits of BYOD practices for both organizations as well as for employees. During data analysis, it is found that allowing the employees to bring their own devices such as smartphones, and tablets brought positive impacts on employee satisfaction. Previously, the businesses around the globe provided company owned devices that increased costs for companies. Moreover, the employees had to carry multiple devices for both work and personal usage. The recent trend of BYOD enabled the employees to use a single device for their personal and work related usage.

Along with this, it is also found from sampled data that BYOD practices increased the productivity of employees in various ways. The employees look after the maintenance of their own devices. Moreover, a higher level of mobility is attached to the BYOD practices since the personal devices of employees are always with them wherever they go. They have access to the Internet all the time during working hours as well as afterwards. This trend enabled employees to respond quicker than before for their work related issues. Through BYOD practices, employees are connected all the time to their personal lives as well as with their organization. In addition to the benefit of raising the level of satisfaction among employees, BYOD practices allowed the companies to attract new talent. In regard to the flexibility of work-from-home practices, it benefits from BYOD practices and is found to be a major selling point for organizations in order to hire new workers. In one of the sampled studies, it is mentioned that new applicants are attracted towards such companies that allow them to work freely from home with the use of their own computers and other devices.

It is also found from the sampled studies that despite the various challenges and risks associated with the use of personal devices at work, organizations are more than willing to allow their employees to bring their own devices at work as the companies realize the importance of the associated benefits. The most important benefit found for the organizations is the cost saving factor. Previously, the companies have to buy cell phones along with call and data packages for their employees that used to cost them a considerable amount on a monthly basis however the rising trend of BYOD practices eliminated these costs for the companies. The fact that big giants such as IBM and various other companies around the globe have allowed their employees to bring their own devices at work speaks about the popularity of these practices. All of these benefits are identified from a keen analysis of sampled studies. Figure 8 shows the model of the identified benefits from the thematic content analysis of the sampled data through NVivo.

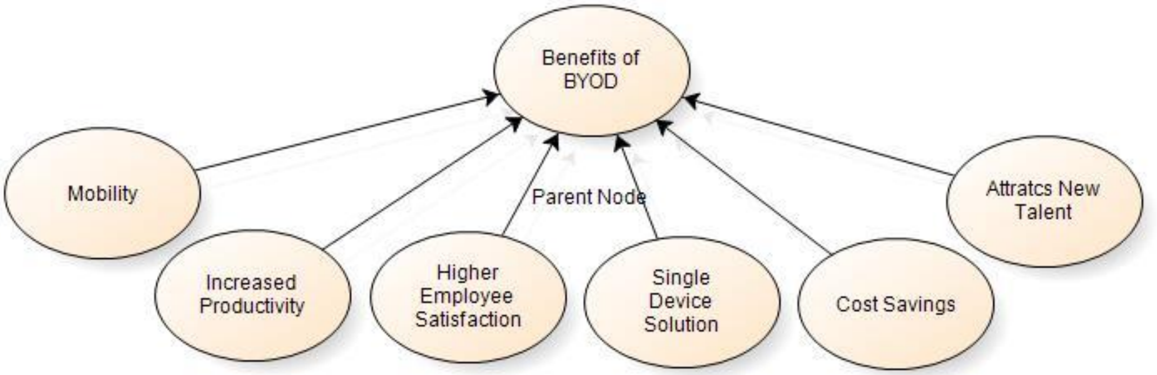

Figure 8: Model for Benefits of BYOD

Text Search Query - Results Preview

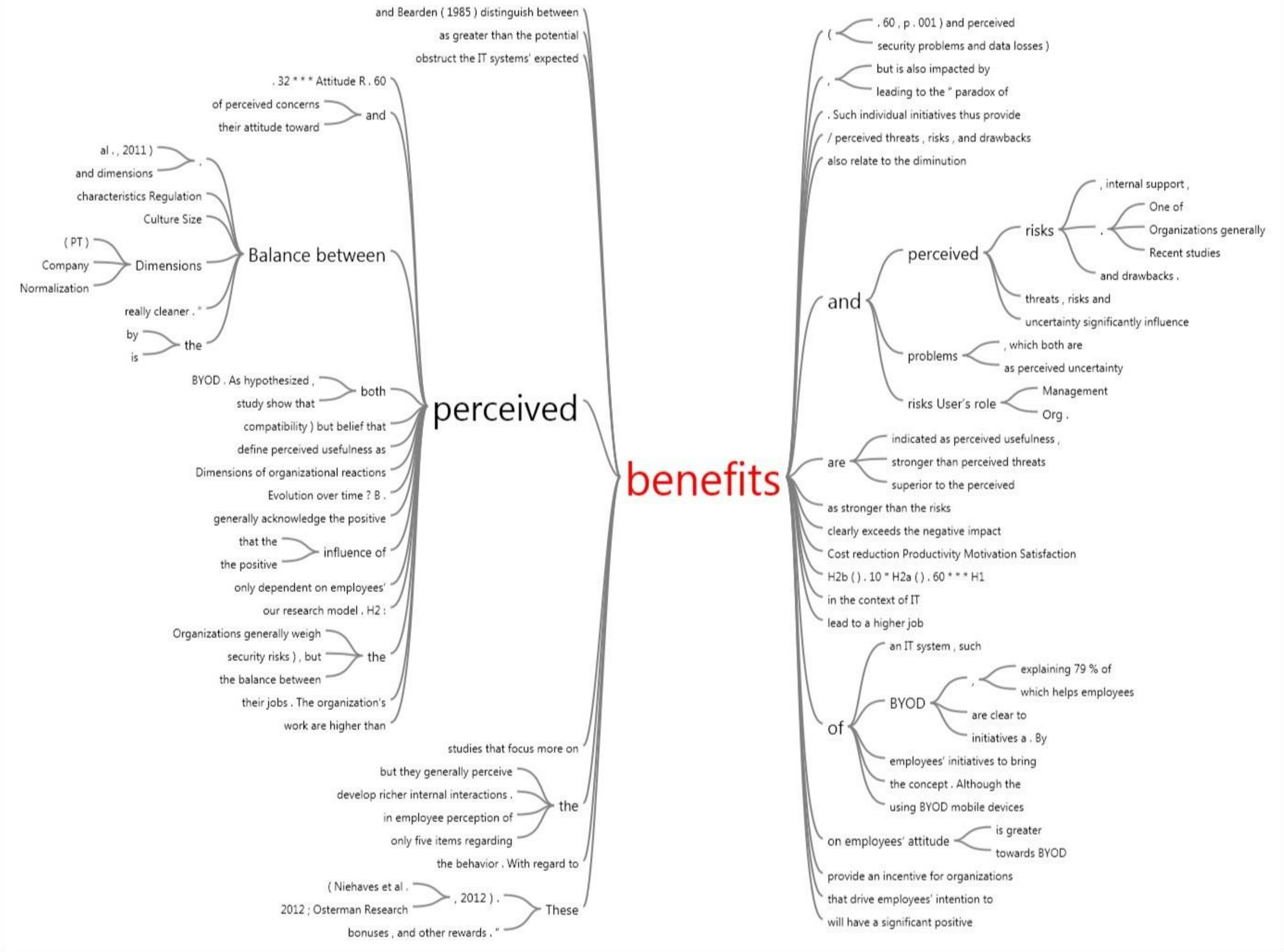
and Bearden (1985) distinguish between
as greater than the potential
obstruct the IT systems' expected
. 32 * * * Attitude R . 60
of perceived concerns
their attitude toward
and
al . , 2011)
and dimensions
,
characteristics Regulation
Culture Size
(PT)
Company
Normalization
Dimensions
Balance between
really cleaner . "
by
is
the
BYOD . As hypothesized ,
study show that
both
compatibility) but belief that
define perceived usefulness as
Dimensions of organizational reactions
Evolution over time ? B .
generally acknowledge the positive
that the
the positive
influence of
only dependent on employees'
our research model . H2 :
Organizations generally weigh
security risks) , but
the balance between
the
their jobs . The organization's
work are higher than
perceived
studies that focus more on
but they generally perceive
develop richer internal interactions .
in employee perception of
only five items regarding
the
the behavior . With regard to
(Niehaves et al .
2012 ; Osterman Research
, 2012) .
bonuses , and other rewards . "
These
benefits
(
. 60 , p . 001) and perceived
security problems and data losses)
,
but is also impacted by
leading to the " paradox of
. Such individual initiatives thus provide
/ perceived threats , risks , and drawbacks
also relate to the diminution
and
perceived
risks
, internal support ,
,
One of
Organizations generally
Recent studies
and drawbacks .
threats , risks and
uncertainty significantly influence
problems
, which both are
as perceived uncertainty
risks User's role
Management
Org .
are
indicated as perceived usefulness ,
stronger than perceived threats
superior to the perceived
as stronger than the risks
clearly exceeds the negative impact
Cost reduction Productivity Motivation Satisfaction
H2b ( ) . 10 * H2a ( ) . 60 * * * H1
in the context of IT
lead to a higher job
of
an IT system , such
BYOD
,
explaining 79 % of
which helps employees
are clear to
initiatives a . By
employees' initiatives to bring
the concept . Although the
using BYOD mobile devices
on employees' attitude
is greater
towards BYOD
provide an incentive for organizations
that drive employees' intention to
will have a significant positive

Figure 9: Text Search Query for Benefits

After running the text search query on the sampled data through NVivo, it is found that there must be balance between the benefits and challenges associated with BYOD practices, as shown in Figure 9. If there is an imbalance between the challenges and benefits then it could create problems for the organization. Figure 9 also highlights that the benefits of BYOD practices are greater than the risks and challenges. Moreover, the value of benefits exceeds the number of problems caused by BYOD deployment. At another point, the figure 9 pointed out that the perceived benefits of BYOD deployment is stronger and exceeds the negative impact caused by BYOD in the organizations. It also enables employees to work freely at any time since their devices are with them all the time. The results pointed out a suggestion that the companies must have strong policies and strategies for BYOD in order to gain more benefit from BYOD deployment.

4.6. Organizational Policies for BYOD Practices

The third and one of the most important themes found from the sampled data is the organizational policy for BYOD practices. The core policy standpoints identified from the sampled data can be seen from figure 10. This figure basically provides the determinants of BYOD policy.

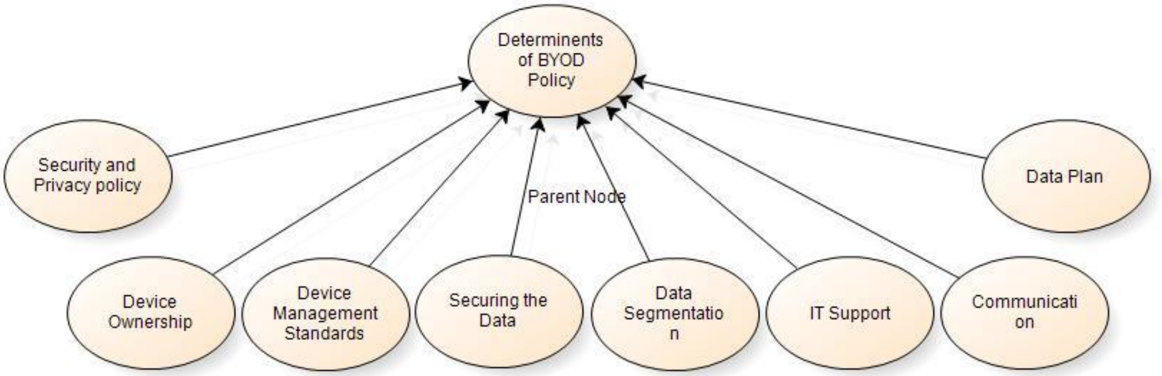

Figure 10: Model for Determinants of BYOD Policy

The deeper analysis of sampled studies highlighted that the organizations must develop such a strategy for their employees, which will enable IT staff to come up with appropriate incident reporting and an acceptable use policy. Moreover, the company must get a signed consent form from all employees in order to get assurance of abiding company's rules and regulations before authorizing them the access of corporate information and sensitive data. Along with this, there must be a centralized device management tool in the organization that can enforce security controls and have features such as password locking unauthorized data and restricting applications.

The policy for BYOD practices should control not only unauthorized access over corporate information, but should also control and secure the data on the personal devices of the employees. This means that the system must be able to erase any stored data on the personal devices of end-users. At the same time, the system must separate the personal data from corporate data, which is a very challenging task. Moreover, the organization must ensure timely IT support in order to cater for any problem or flaws and furthermore the IT department must conduct training sessions for employees for efficient and productive use of personal devices. The company sponsored data plans must be strictly monitored, so that it can be assessed how much of the data was used personal reasons and how much for official work-related business. One way of doing this could be by using dual SIM devices, so that employees could use their work mobile plans for their work and personal mobile plans for personal data. In the end, the BYOD policy must be communicated to each and every user/employee throughout the organization so that everyone would be aware of the set rules and regulations.

The policy implications can also be viewed from a different perspective in Figure 11 and this shows that the company must have a policy to incorporate a secure device management tool. Moreover, there must be clear policies to restrict the unauthorized release of data and information. The main policy must cater for the challenges, issues, and security threats associated to BYOD deployment. All the themes mentioned above helped in identifying the major issues that prevailed in the sampled reports, articles, and case studies. It also provided a deeper insight into the published material in this field of research. Although the issues related to BYOD practices are gaining attention from organizations and researchers this issue requires more research.

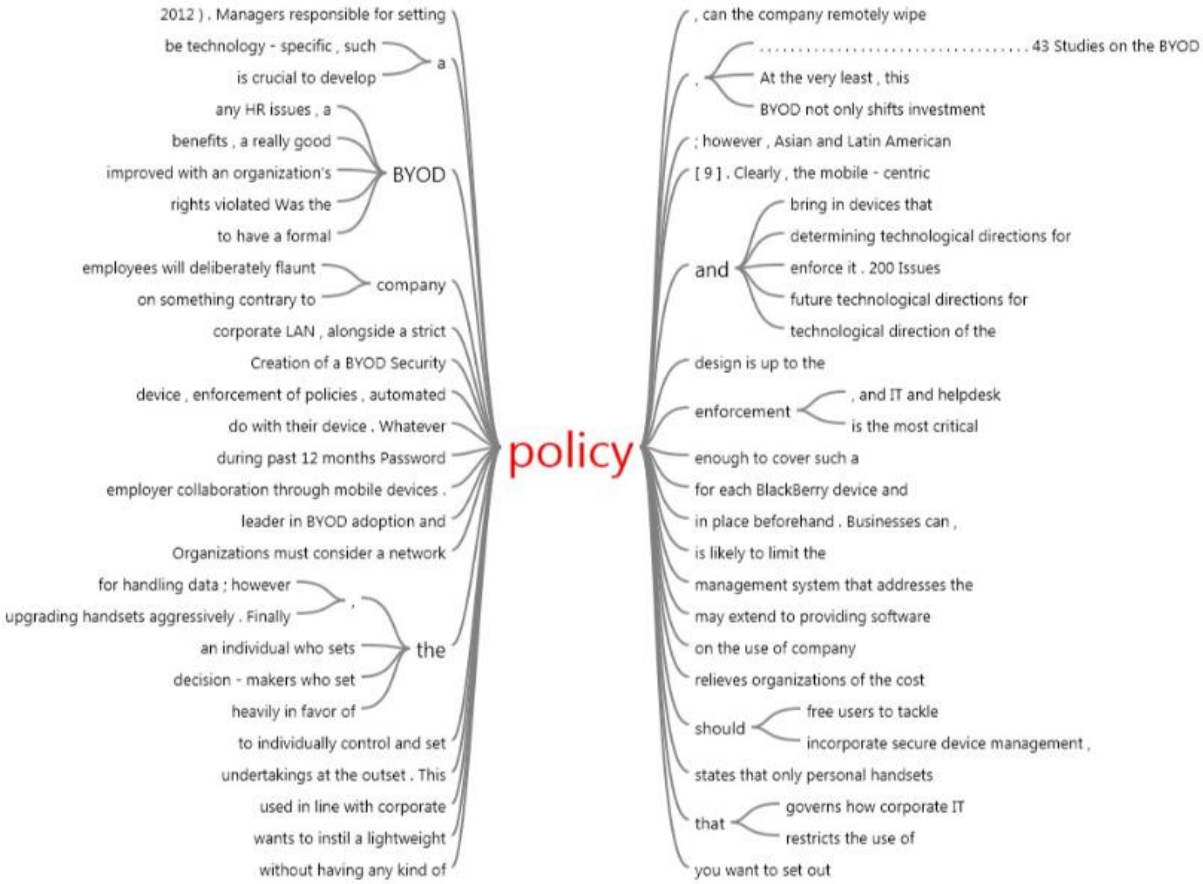
2012) . Managers responsible for setting
be technology - specific , such
is crucial to develop
a
any HR issues , a
benefits , a really good
improved with an organization's
rights violated Was the
to have a formal
BYOD
employees will deliberately flaunt
on something contrary to
company
corporate LAN , alongside a strict
Creation of a BYOD Security
device , enforcement of policies , automated
do with their device . Whatever
during past 12 months Password
employer collaboration through mobile devices .
leader in BYOD adoption and
Organizations must consider a network
for handling data ; however
upgrading handsets aggressively . Finally
,
an individual who sets
decision - makers who set
heavily in favor of
the
to individually control and set
undertakings at the outset . This
used in line with corporate
wants to instil a lightweight
without having any kind of
policy
, can the company remotely wipe
.
..................................43 Studies on the BYOD
At the very least , this
BYOD not only shifts investment
; however , Asian and Latin American
[9] . Clearly , the mobile - centric
and
bring in devices that
determining technological directions for
enforce it . 200 Issues
future technological directions for
technological direction of the
design is up to the
enforcement
, and IT and helpdesk
is the most critical
enough to cover such a
for each BlackBerry device and
in place beforehand . Businesses can ,
is likely to limit the
management system that addresses the
may extend to providing software
on the use of company
relieves organizations of the cost
should
free users to tackle
incorporate secure device management ,
states that only personal handsets
that
governs how corporate IT
restricts the use of
you want to set out

Figure 11: Text Search Query for Policy

An analysis of Figure 11 indicates that BYOD policies focus on issues of control, restrictions, violations, and limitations. These point to an agency theory focus, the dominant perspective among managers. Little is said about concepts such as, mutual benefits, shared governance, and cooperation, which would point towards a stewardship view. Thus, the dominant perspective of BYOD policies is to consider the agentic responsibilities of employees.

4.7. Conclusion

This chapter identified the major issues related to BYOD and the remaining areas for research. The next chapter comprises the discussion, the overall conclusions, limitations of the study, and suggestions for further research.

Chapter 5: Discussion and Conclusion

5.1. Discussion

This study set out to review BYOD management practices and policies used by organisations and to explore how the interests of employees and employers can be balanced.

To discuss the research questions, a thematic content analysis was conducted through a qualitative approach using secondary data. The first theme that can be extracted from the findings is that BYOD practices do not only affect the employees but also affect the working environment. As the employees use their mobile devices to perform their job, there are many risks and threats associated with it and that has raised various challenges for the organisations around the world. The benefit to senior management of using personal devices has introduced more challenges to the IT department in the workplace over the control of the sensitive data.

The second theme found various challenges associated with BYOD practices such as security threats, privacy issues, social issues and technological complexities. It is very important to mention that an awareness and familiarity with the challenges of BYOD practices can help employees understand some critical areas associated with the use of personal devices, as well as help organizations enhance their information security. Five concerns were found to be important in BYOD practices such as physical access of personal devices, loss and theft of devices, end-user device ownership, lack of awareness from employee's side, and increasing desire for data access. Both employees as well as organizations need to cater for these concerns in order to have a secure environment at the workplace.

There is another challenge/risk in terms of privacy in front of companies during BYOD deployment. It becomes very easy for the IT department to keep track of employee’s location with the help of company-installed applications on employee’s personal devices. This practice is illegal in certain countries. Moreover, ensuring the regulatory compliance in BYOD policies is another challenge for organizations related to certain industries such as healthcare and financial institutions. The most common challenge for organizations in the case of BYOD practices is the loss and theft of personal devices at workplace. This challenge is found in almost every sampled study. And finally, the challenge associated to BYOD deployment is ensuring the timely data recovery. Organizations face lots of difficulties in recovering and wiping out the unauthorized data from the end-user’s personal device.

Other than the challenges mentioned above, the greatest challenge for an organization is the legal ownership of the data that is stored in the personal devices of employees. The development of certain policies and strategies for ensuring the legal ownership is the area in which various organizations are struggling nowadays. Defining and determining the most appropriate policy is found to be a crucial task for organizations in recent times. The insight analysis of sampled resources also highlighted the direct implications of enterprise access on helpdesk resources, network/device control, firm security, and information ownership.

The third theme is about the benefits of BYOD practices. The benefit of extended mobility due to BYOD provides more flexibility. In addition, the freedom of choice regarding work contributes to the happiness of knowledge workers. When an organization adopts an open workplace policy that allows employees to get their work done from wherever they want to do it, the organization must also identify their management needs regarding network security. Moreover, if employees fund their own devices, BYOD may have an even more positive effect on a company as the employee makes a capital investment that benefits the company, and reduces the IT cost for the organizations. These are some of the benefits, which call for the need for BYOD practices and recommend that organizations allow their employees to bring their own devices at their workplace.

While there many benefits of BYOD practices, there are also some threats associated with it. The major sources of attacks on mobile devices include hackers, foreign governments, cybercriminals, botnet operators, terrorists, and spy-agencies. Cybercrimes, such as obtaining sensitive or private data, money, and intellectual property are threats faced by all types of organizations.

All of these threats are forcing organizations to come up with a solution and also to develop an appropriate BYOD policy. The review of material on BYOD found that there is no consensus over a single software or program for combating all of the threats associated to mobile devices. Users are seen as the weakest link in the majority of the systems and the security system is highly dependent upon this weakest link. Many research studies pointed out the risk in using public Wi-Fi networks and exposure to unknown web links. Moreover, the installation of suspicious apps, software and programs must also be avoided in case of any potential security exploitation.

The fourth and one of the most important themes found is the organizational policy for BYOD practices. It is found from the data analysis that the organization must prepare an assessment of the pros and cons of any proposed BYOD deployment. If the pros are found to be more than the cons then in that case the organization should allow the usage of personal devices at work. The organization must also assess their capacity to manage the risks associated to BYOD deployment. The deeper content analysis of sampled data pointed out that it should be organization's top most priority to protect the sensitive and valuable information in shape of organization's intellectual property by making data security plan. In order to counter security threats, the company must initiate a layered security strategy, which would be capable enough to provide only the authorized access to corporate information by minimizing the chances of any type of theft and other risks. The results highlighted the strategies such as frequent log analysis, security solutions, and efficient audit logging in order to protect the sensitive corporate information.

Some other important points for BYOD policy are also found from the data analysis. These include the implications of granting enterprise access to personal devices and the sensitive information located in them. These include the assurance of keeping the company's core network malware-free, having a clear understanding of the content present on the network, the identity of end-users, determining the type and level of information that can be stored on the network, and maintaining an audit and compliance process in regard to the requirements set by the proper enforcement of access policies.

With respect to BYOD policies, a stewardship approach, in contrast to an agency approach, would be predicated on creating internal governance mechanisms in which the rights of employees and employers are protected, in such a manner that those rights are underscored by responsibilities and duties to be upheld by both parties for everyone's mutual benefit. In contrast, policies based on agency theory would focus addressing the prevention of loss due to divergent principal and agent goals. In general, both agency and stewardship theories maintain that equilibrium between employees and employers or perhaps more appropriately, employees and managers/supervisors, can be achieved and maintained under certain circumstances. In particular, this typically involves ensuring that both parties act to increase their own independent and interdependent utility.

5.2. Conclusion

This research study was aimed to have a better understanding about the rising issue of BYOD practices and policies adopted by various organizations around the globe. Moreover, the advantages and disadvantages of BYOD practices for employees and organizations are also discussed as well as balancing the interests of employees and employers using agency and stewardship theories.

To answer the research questions and achieve the research objectives, a qualitative study was conducted. The qualitative research approach was ~~all~~ based on thematic content analysis of most of the material published in electronic journals, and from the annual reports of companies around the globe. For a better understanding of the data, NVivo was applied on sampled material. The results of the study indicated that the issue of BYOD has only recently attracted the attention of researchers and practitioners as most of the research has been conducted from 2010 onwards. Thus, the issue of BYOD requires much more effort to be resolved.

Moreover, the results also highlighted some of the risks and threats associated to BYOD practices such as security threats, privacy issues, social issues, and technological complexities. In addition to this, the results also highlighted that the terms such as security problems, technological complexities, organizational policy, employees, and data issues have a higher number of coding references and most of the research is conducted in these areas. The deeper analysis of the data also concludes that the issue of BYOD is not only faced by management sciences, but also influences upon other fields such as engineering, and IT.

Moreover, the interests of employees and employers when implementing BYOD can be balanced when there are explicit plans and policies from the organisation to gain win-win situation. When developing the policy, it is important to take both employee expectations and employers view into account and make sure the policy is practical. BYOD policy is a particular policy that enables IT departments in organisations to increase their control over the organisation's data and information.

This study also concludes that policy making for BYOD practices still requires lots of effort and there is much to be achieved by organizations in establishing an environment that will be beneficial for both employees and organizations. Some of the major concerns related to BYOD practices, such as access to personal devices, the loss and theft of devices, end-user device ownership, a lack of awareness by employees, and an increasing interest in data access, require more effort from IT personnel to maintain a secure working environment. Organisations engaging in BYOD have to examine how the benefits and drawbacks balance in their own contexts.

5.3. Limitations of Study

This is one of the very few full-fledged research studies on the issue of BYOD practices and policy implications. Thus, some of the limitations are natural. The first and most prominent limitation of this study is associated with the research approach. This study was based on secondary data. There was no use of primary material from employees or managers. Thus, the opinions of stakeholders on this issue were not gathered. Another limitation of this study is limiting the search to English-language publications. It is possible that if I had obtained articles on organisations in countries which are intensive users of mobile devices but use languages other than English, such as China, India, France and Germany, the results of the review may be different.

5.4. Recommendations for Future Research

Future researchers should obtain primary data on the BYOD trend by surveying and interviewing stakeholders in organisations, such as employees, functional managers, IT managers, and senior management. The results of this study can be used to develop concepts for a quantitative study to enhance our understanding of the issue by gathering data from a broader sample of actual users. In addition, the issue can be explored in other cultural and national contexts to improve the generalizability of the findings.

References

AirWatch. (2012). *Enabling bring your own device (BYOD) in the enterprise.* Retrieved from: http://www.ciosummits.com/media/solution_spotlight/byod-whitepaper.pdf

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). *Information Security Policy Compliance: The Role of Information Security Awareness.* Proceedings of the 2012 Americas' Conference on Information Systems (AMCIS). Retrieved from http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/16/

Ardichvili, A., Jondle, D., Kowske, B., Cornachione, E., Li, J., & Thakadipuram, T. (2012). Ethical cultures in large business organizations in Brazil, Russia, India, and China. *Journal of Business Ethics, 105*(4), 415-428.

Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Securing the Bring Your Own Device Paradigm. *Computer, 47*(6), 48-56.

Aycan, Z., Schyns, B., Sun, J. M., Felfe, J., & Saher, N. (2013). Convergence and divergence of paternalistic leadership: A cross-cultural investigation of prototypes. *Journal of International Business Studies, 44*(9), 962-969.

Barnes, N. M. (2013). BYOD: balancing employee privacy concerns against employer security needs. Lexology. Retrieved 30 October 2015 http://www.lexology.com/library/detail.aspx?g=1109490a-6895-40f0-a7a3-afc714316165

Belle, S. M. (2015). Knowledge Stewardship as an Ethos-Driven Approach to Business Ethics. *Journal of Business Ethics*, 1-9.

Berg, B. L. (2007). *Qualitative Research Methods for the Social Sciences* (7th ed.): Allyn & Bacon.

Berry, A. J., & Otley, D. T. (2004). Case-based research in accounting. *The real life guide to accounting research*, 231-55.

Bertoncini, G., Griesert, C., & Magette, R. (2012). Stewardship theory. Retrieved 30 October 2015 https://www.academia.edu/4371638/Stewardship_Theory

Bogdan, R., & Biklen, S. K. (1992). *Qualitative Rsearch for Education*. Boston: Allyn and Bacon.

Botnet. (n.d.).How a botnet works. In *Wikipedia*. Retrieved October 14, 2015, from https://en.wikipedia.org/wiki/Botnet. Reprinted with permission.

Boussebaa, M., Sturdy, A., & Morgan, G. (2014). Learning from the world? Horizontal knowledge flows and geopolitics in international consulting firms. *The International Journal of Human Resource Management, 25*(9), 1227-1242.

Boyles, J. L., Smith, A., & Madden, M. (2012). Privacy and data management on mobile devices.   Retrieved 20 August, 2015, from http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Bryman, A. (2001). *Social Research Methods*: Oxford University Press.

Calder, A. (2013). Is the BYOD Movement Worth the Risks. *Credit Control Journal, 34*, 65-69.

Chiva, R., & Habib, J. (2015). A Framework for Organizational Learning Types: Generative, Adaptive and Zero Learning. *Journal of Management & Organization, 21*(3), 350-368.

CISCO. (2014). *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update*, 2014–2019: CISCO Systems.

Corbetta, G., & Salvato, C. (2004). Self-Serving or Self Actualizing? Models of Man and Agency Costs in Different Types of Family Firms: A Commentary on Comparing the Agency Costs of Family and Non-Family Firms: Conceptual Issues and Exploratory Evidence. *Entrepreneurship Theory and Practice, 28*(4), 355–362.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Creswell, J. W. & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory into Practice*, 39(3), 124-131.

Davis, J. H., Schoorman, F. D., & Donaldson, L. (1997). Davis, Schoorman, and Donaldson Reply: The Distinctiveness of Agency Theory and Stewardship Theory. *Academy of Management Review*, *22*(3), 611-613.

Denzin, N., & Lincoln, Y. (2004). *Handbook for Qualitative Research*. California: Sage Publications.

Dernbecher, S., Beck, R., & Weber, S. (2013). *Switch to Your Own to Work with the Known: An Empirical Study on Consumerization of IT*. Proceedings of the 2013 Americas' Conference on Information Systems (AMCIS). Retrieved from http://aisel.aisnet.org/amcis2013/EndUserIS/GeneralPresentations/9/

Donaldson, L., & Davis, J. H. (1991). Stewardship theory or agency theory: CEO governance and shareholder returns. *Australian Journal of management, 16*(1), 49-64.

Etsebeth, V. (2011). Defining the current corporate IT risk landscape. *Journal of International Commercial Law & Technology*, *6*(2), 62-73.

Fox, M. A., & Hamilton, R. T. (1994). Ownership and diversification: Agency theory or stewardship theory. *Journal of Management Studies, 31*(1), 69-81.

Freedman, T. (2012). BYOD case study: George Spencer Academy. ICT in Education. Retrieved July 15, 2015 from http://www.ictineducation.org/home-page/2012/10/31/byod-case-study-george-spencer-academy.html .

Frith, H., & Gleeson, K. (2004). Clothing and embodiment: men managing body image and appearance. *Psychology of Men & Masculinity, 5*(1), 40-48.

GAO. (2012). Information security: Better implementation of controls for mobile devices should be encouraged.   Retrieved 10 August, 2015, from http://www.gao.gov/assets/650/648519.pdf

Gavetti, G. (2012). Perspective- Toward a behavioral theory of strategy. *Organization Science, 23*(1), 267-285.

Goyder, M. (2011). Family Matters *Financial Management* (pp. 63).

Gu, G., Zhang, J., & Lee, W. (2008). BotSniffer: Detecting botnet command and control channels in network traffic. *Proceedings of the 15th Annual Network and Distributed System Security Symposium*. Retrieved from: http://corescholar.libraries.wright.edu/cse/7

Harris, S. (2010). Access control. In J. Jue & R. Bart (Eds.), *CISSP all-in-one exam guide* (5th ed., pp. 153–279). New York, NY: McGraw-Hill.

Hennink, M., Hutter, I., & Bailey, A. (2011). *Qualitative research methods*. Sage.

Hernandez, M. (2012). Toward an understanding of the psychology of stewardship. *Academy of Management Review, 37*(2), 172-193.

Hinkes, A. (2013). BYOD Policies: A Litigation Perspective. *Corporate Counsel Litigation, 27*(2).

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences, 43*(4), 615-660.

Hunt, J. (2012). BYOD Policy–What Businesses Need to Consider. *Credit Control, 33*(5), 6.

Jansen, W., & Scarfone, K. (2008). Guidelines on cell phone and PDA security R*ecommendations of the National Institute of Standards and Technology* (NIST SP800–124). Retrieved 20 August, 2015, from http://csrc.nist.gov/publications/nistpubs/800–124/SP800–124.pdf

Jensen, M. C., & Smith, C. W. (2000). Stockholder, manager, and creditor interests: applications of agency theory. *Theory of the Firm, 1*(1).

Jindal, A. K. (2013). *Protecting Android Devices Following BYOD Policy against Data Security and Privacy Attacks*. (M.Tech thesis), New Delhi. Retrieved from https://repository.iiitd.edu.in/jspui/handle/123456789/105

Johnson, B., & Christensen, L. (2004). *Educational research: Quantitative, qualitative, and mixed approaches*. Boston: Allyn and Bacon.

Jonker, J. and Pennink, B. (2010), *The Essence of Research Methodology: A Consice Guide for Master and PhD Students in Management Science*, Springer, Heidelberg.

Kissel, R. (2012). Glossary of key information security terms (draft). USA, *National Institute of Standards and Technology*, DOI: http://dx. doi. org/10.6028/NIST. IR, 7298.

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics, 33*, 159- 174.

Le Grand, C. H. (2013). Positive Security, Risk Management, and Compliance. *EDPACS, 47*(4), 1-10.

Lebek, B., Degirmenci, K., & Breitner, M. H. (2013). *Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices*.

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

Liu, L., Moulic, R., & Shea, D. (2010). *Cloud service portal for mobile device management.* Paper presented at the IEEE Seventh International Conference on E-Business Engineering

Loose, M., Gewald, H., & Weeger, A. (2013). *Examining the Determinants of BYOD Service Adoption Behavior*. Chicago, Illinois.

Marshall, S. (2014). IT consumerization: A case study of BYOD in a healthcare setting. *Technology Innovation Management Review*, *4*(3).

Mahesh, S., & Hooter, A. (2013). Managing and securing business networks in the smartphone era *Management Faculty Publications, Paper 5*. Retrieved from http://scholarworks.uno.edu/mgmt_facpubs/5

Microsoft. (2006). Windows mobile device management and security solutions guide. Retrieved 20 August, 2015, from http://www.microsoft.com/windowsmobile

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security considerations. *IT Pro*, 53-55.

Mont, M. C., & Brown, R. (2011). *Risk assessment and decision support for security policies and related enterprise operational processes.* Paper presented at the IEEE International Symposium on Policies for Distributed Systems and Networks.

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, 5-8.

Niehaves, B., Köffer, S., Ortbach, K., & Katschewitz, S. (2012). Towards an IT consumerization theory–a theory and practice review. Working chapters. *European Research Center for Information Systems, 13*.

Neuman, W. L. (2011). *Social work research methods: Qualitative and quantitative approaches*. Allyn and Bacon.

Nord, W. R. (1969). Beyond the teaching machine: The neglected area of operant conditioning in the theory and practice of management. *Organizational Behavior and Human Performance, 4*(4), 375-401.

ODNI. (2012). How intelligence works.   Retrieved 20 August, 2015, from http://www.intelligence.gov/about-theintelligence-community/how-intelligence-works/data-gathering.html

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open*, 1–11.

Ortbach, K., Köffer, S., Bode, M., & Niehaves, B. (2013). *Individualization of Information Systems*.

Patton, M. Q. (1990). *Qualitative evaluation and research methods* (2nd ed.). Newbury Park, CA: Sage.

Phillips, E. (2014). Changing Dimensions of Privacy in the Workplace: Legal Rights and Labour Realities, The. *Canadian Lab. & Emp. LJ*, *18*, 467.

Regard, D. L. (2012). Mobile devices: Catalyst for better records management? *Information Management Journal, 46*(5), 10-12.

Ritchie, J., & Lewis, J. (Eds.). (2003). *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. London: Sage Publications

Rose, C. (2012). Smart phone, dumb security. *Review of Business, 16*(1), 21-26.

Ruggiero, P., & Foote, J. (2011). *Cyber Threats to Mobile Phones: United States Computer Emergency Readiness Team.*

Saunders, M. L., & Lewis, P. (2000). P. and Thornhill, A.(2009), Research Methods for Business Students. *Financial Times Prentice Hall Inc., London*.

Scarfo, A. (2012, November). New security perspectives around BYOD. In *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on* (pp. 446-451). IEEE.

Scarfone, K., & Souppaya, M. (2012). Guidelines for managing and securing mobile devices in the enterprise: *Recommendations of the National Institute of Standards and Technology* (SP800–124 Rev. 1). Manuscript in preparation. Retrieved 20 August, 2015, from http://csrc.nist.gov/publications/drafts/800–124r1/draft_sp800–124-rev1.pdf

Schorn, A. (2000). The "Theme-centered Interview". A Method to Decode Manifest and Latent Aspects of Subjective Realities. *FQS, 1*(2), 1-9.

Schultz, E. E., & Shpantzer, G. (2010). Information security management handbook. In H. F. Tipton & M. K. Nozaki (Eds.), *Security* (pp. 107–125). Boca Raton, FL: BCRC Press.

Seale, C. (1999). Quality in qualitative research. *Qualitative Inquiry,* 5(4), 465-478.

Shapiro, S. P. (2005). Agency theory. *Annual review of sociology*, *31*(1), 263-284.

Singhal, S. (2002). Top 10 Vulnerabilities in Today's Wi-Fi Networks. Retrieved 30 October, 2015, from http://www.computerworld.com/article/2577244/security0/top-10-vulnerabilities-in-today-s-wi-fi-networks.html

Smith, J. A., & Osborn, M. (2003). Interpretative phenomenological analysis. In J. A. Smith (Ed.), *Qualitative Psychology: A Practical Guide to Methods*: Sage Publications.

Stalling, W., Brown, L., Bauer, M., & Howard, M. (2008). Malicious software BOTS. In T. Dunkelberger & C. Snyder (Eds.), *Computer Security: Principles and Practice* (pp. 215–248). Upper Saddle River, NJ: Pearson Prentice Hall.

Taiple, K. (2012). Overview: What is cybercrime? Retrieved 20 August, 2015, from http://www.information-retrieval.info/cybercrime/index01.html

Thomson, G. (2012). BYOD: enabling the chaos. *Network Security, 2*, 5-8.

Vallejo, M. C. (2009). The Effects of Commitment of Non-Family Employees of Family Firms from the Perspective of Stewardship Theory. *Journal of Business Ethics, 87*, 379-390.

Vandelannoitte, A. L.-. (2015). Managing BYOD: how do organizations incorporate user-driven IT innovations? *Information Technology & People, 28*(1), 2-33.

Viega, J., & Michael, B. (2010). Mobile device security. *IEEE Security & Privacy*, 11-12.

Walker, M. (2012). Glossary. In T. Green (Ed.), *CEH Certified Ethical Hacker Exam Guide* (pp. 339–371). New York, NY: McGraw-Hill.

Weber, R. P. (1990). *Basic Content Analysis*: Sage Publishers.

Wilson, C. (2008). *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for Congress (CRS Report RL32114)*. Retrieved 20 August, 2015, from http://www.fas.org/sgp/crs/terror/RL32114.pdf

Wiseman, R. M., Cuevas-Rodríguez, G., & Gomez-Mejia, L. R. (2012). Towards a social theory of agency. *Journal of Management Studies, 49*(1), 202-222.

Zimmerman, A. S., & Szenberg, M. (2000). Implementing international qualitative research: techniques and obstacles. *Qualitative Market Research: An International Journal, 3*(3), 158-164.

Appendices

Appendix 1: Results of Database Searches

Database	Search term	Number of Hits /Results
ABI/Info ProQuest	BYOD	510
	Bring your own devices at workplace	1532
	organization policies for BYOD	41
	BYOD & Gover* & polic*	58
	impact of BYOD on employee satisfaction and performance	9
Emerald Insight	BYOD	41
JSTOR	BYOD	15
ProQuest research library	BYOD	1,940
	BYOD & polic*	74
	BYOD & polic* & gover*	7
	Bring your own device	254
	Cost related issues to BYOD	26
	Bring your own device & polic*	65
	Case study of BYOD	45
Sage Journals	BYOD	20
	Impact of BYOD on employee satisfaction and performance	4
	Advantages of BYOD policy	10
	organization policies for BYOD	9
Scopus	BYOD	215
	Organization policies for BYOD	27
	Bring your own device	183
SpringerLink	BYOD	519
Taylor & Francis	BYOD	81
	Case study of BYOD	65
	Advantages of BYOD policy	27
Web of Science	BYOD	49
Willey Online Library	BYOD	81
	Issues related to BYOD policies	32

<u>Note:</u>

- *The search term "gover*" was used to find documents that included terms such as "governance" that begin with the word stem "gover".*
- *The search term "polic*" was used to find documents that included terms such as "policy" that begin with the word stem "polic".*

Appendix 2: List of Studies Used for Review

No.	Full Reference
1	AirWatch. (2012). Enabling bring your own devices (BYOD) in the enterprise. http://www.ciosummits.com/media/solution_spotlight/byod-whitepaper.pdf
2	Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). *Information Security Policy Compliance: The Role of Information Security Awareness.* Proceedings of the American Conference on Information Systems (AMCIS).
3	Ardichvili, A., Jondle, D., Kowske, B., Cornachione, E., Li, J., & Thakadipuram, T. (2012). Ethical cultures in large business organizations in Brazil, Russia, India, and China. *Journal of Business Ethics, 105*(4), 415-428.
4	Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Securing the Bring Your Own Device Paradigm. *Computer, 47*(6), 48-56.
5	Barnes, N. M. (2013). BYOD: balancing employee privacy concerns against employer security needs. Retrieved 30 October 2015 http://www.lexology.com/library/detail.aspx?g=1109490a-6895-40f0-a7a3-afc714316165
6	Belle, S. M. (2015). Knowledge Stewardship as an Ethos-Driven Approach to Business Ethics. *Journal of Business Ethics*, 1-9.
7	Boyles, J. L., Smith, A., & Madden, M. (2012). *Privacy and data management on mobile devices*. Retrieved 20 August, 2015, from http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx
8	Calder, A. (2013). Is the BYOD Movement Worth the Risks? *Credit Control Journal*, *34*, 65-69.
9	Dernbecher, S., Beck, R., & Weber, S. (2013). *Switch to Your Own to Work with the Known: An Empirical Study on Consumerization of IT*.
10	GAO. (2012). Information security: Better implementation of controls for mobile devices should be encouraged. Retrieved 10 August, 2015, from http://www.gao.gov/assets/650/648519.pdf
11	Harris, S. (2010). Access control. In J. Jue & R. Bart (Eds.), *CISSP all-in-one exam guide* (5th ed., pp. 153–279). New York, NY: McGraw-Hill.
12	Hinkes, A. (2013). BYOD Policies: A Litigation Perspective. *Corporate Counsel Litigation*, *27*(2).

13	Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences, 43*(4), 615-660.
14	Jansen, W., & Scarfone, K. (2008). *Guidelines on cell phone and PDA security recommendations of the National Institute of Standards and Technology (NIST SP800–124).* Retrieved 20 August, 2015, from http://csrc.nist.gov/publications/nistpubs/800–124/SP800–124.pdf
15	Lebek, B., Degirmenci, K., & Breitner, M. H. (2013). *Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices*.
16	Liu, L., Moulic, R., & Shea, D. (2010). *Cloud service portal for mobile device management.* Paper presented at the IEEE Seventh International Conference on E-Business Engineering, Shanghai
17	Loose, M., Gewald, H., & Weeger, A. (2013). *Examining the Determinants of BYOD Service Adoption Behavior*. Chicago, Illinois.
18	Mahesh, S., & Hooter, A. (2013). Managing and securing business networks in the smartphone era *Management Faculty Publications, Paper 5, University of New Orleans*. http://scholarworks.uno.edu/mgmt_facpubs/5
19	Marshall, S. (2014). IT consumerization: A case study of BYOD in a healthcare setting. *Technology Innovation Management Review, 4*(3), 14-18.
20	Microsoft. (2006). Windows Mobile Device Management and Security Solutions guide. Retrieved 20 August, 2015, from www.microsoft.com/windowsmobile
21	Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security considerations. *IT Pro*, 53-55.
22	Mont, M. C., & Brown, R. (2011). *Risk assessment and decision support for security policies and related enterprise operational processes.* Paper presented at the IEEE International Symposium on Policies for Distributed Systems and Networks.
23	Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, 5-8.
24	New BYOD service bridges gap. (2011). *International Journal of Micrographics & Optical Technology, 29*(6), 15.
25	ODNI. (2012). How intelligence works. Retrieved 20 August, 2015, from http://www.intelligence.gov/about-theintelligence-community/how-intelligence-works/data-gathering.html

26 Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open*, 1–11.

27 Regard, D. L. (2012). Mobile devices: Catalyst for better records management? *Information Management Journal, 46*(5), 10-12.

28 Rose, C. (2013). BYOD: An examination of bring your own device in business. *The Review of Business Information Systems (Online), 17*(2), 65.

29 Rose, C. (2012). Smart phone, dumb security. *Review of Business, 16*(1), 21-26.

30 Ruggiero, P., & Foote, J. (2011). *Cyber Threats to Mobile Phones*, United States Computer Emergency Readiness Team.

31 Scarfone, K., & Souppaya, M. (2012). *Guidelines for managing and securing mobile devices in the enterprise: Recommendations of the National Institute of Standards and Technology* (SP800–124 Rev. 1). Retrieved 20 August, 2015, from http://csrc.nist.gov/publications/drafts/800–124r1/draft_sp800–124-rev1.pdf

32 Schultz, E. E., & Shpantzer, G. (2010). Information security management handbook. In H. F. Tipton & M. K. Nozaki (Eds.), *Security* (pp. 107–125). Boca Raton, FL: BCRC Press.

33 Stalling, W., Brown, L., Bauer, M., & Howard, M. (2008). Malicious software BOTS. In T. Dunkelberger & C. Snyder (Eds.), *Computer security: Principles and practice* (pp. 215–248). Upper Saddle River, NJ: Pearson Prentice Hall.

34 Taiple, K. (2012). Overview: What is cybercrime? Retrieved 20 August, 2015, from http://www.information-retrieval.info/cybercrime/index01.html

35 Thomson, G. (2012). BYOD: enabling the chaos. *Network Security, 2*, 5-8.

36 Vandelannoitte, A. L.-. (2015). Managing BYOD: how do organizations incorporate user-driven IT innovations? *Information Technology & People*, 28(1), 2-33.

37 Vandelannoitte, A. L.-. (2015). Leaving employees to their own devices: new practices in the workplace. *Journal of Business Strategy*, 36(5), 18-24.

38 Viega, J., & Michael, B. (2010). Mobile device security. *IEEE Security & Privacy*, 11-12.

39 Weeger, A., Wang, X., & Gewald, H. (2015). IT Consumerization: BYOD-Program Acceptance and its Impact on Employer Attractiveness. *The Journal of Computer Information Systems, 56*(1), 1-10.

40	Wilson, C. (2008). Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for Congress (CRS Report RL32114). Retrieved 20 August, 2015, from http://www.fas.org/sgp/crs/terror/RL32114.pdf