MASTER'S THESIS

The Benefits and Threats of BYOD in a SME Enterprise

A Systematic Literature Review

Enda Lydon
2014

Master (120 credits)
Master of Science in Information Security

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

LULEÅ UNIVERSITY OF TECHNOLOGY

Luleå Tekniska Universitet of Sweden

The benefits and threats of BYOD in a SME enterprise

A systematic literature review

Enda Lydon

ACKNOWLEDGEMENTS

I would never have been able to finish my thesis without the guidance of my supervisor, my fellow thesis group members, help from my friends, and support from my wife.

I would like to express my deepest gratitude to my academic supervisor, Prof. Helena Karasti, for her excellent guidance, patience, and understanding and for providing me with excellent advice and encouragement to allow me to complete this research.

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

Finally, I would like to thank my wife, Úna, for your love, understanding, patience and support, all of which made it possible for me to bring this research work to an end.

ABSTRACT

In today's current economic climate, companies are always looking for innovative ways to help in their enterprises' business processes. Companies try to adopt new technological trends in order to improve their business in terms of both performance and efficiency, so that they can keep up with the market competition. One of the latest trends is "Bring your own Device" (BYOD). Instead of companies having to provide the required hardware/software to its employees, by adopting BYOD policies, employees are allowed to use their own computers or smart phones at work. Since they are already acquainted with how these devices work, they are inclined to be more productive. The benefits of this lead to higher work satisfaction, and can also help shift some of the costs to the user, which enhances the cost-efficiency of the business.

In order to facilitate this, policies have to be drawn up in order to protect the company's assets and to provide guidelines. However, when Small and Medium sized Enterprises (SME's) try to implement policies and guidelines for BYOD, it becomes more difficult as they usually do not have a dedicated IT Security department to assist them. The question that needs to be answered is how the risks mentioned can be reduced to acceptable levels, in order to support a secure adoption of BYOD in a SME environment.

This thesis presents a systematic literature review (SLR) of published research articles concerning Bring your Own Device in order try to answer this question.

Keywords

Bring your own device (BYOD), Mobile device management, Small & Medium Enterprises (SME's), Computer security, Security considerations, Systematic Review

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 WHAT IS BYOD?

Bring your own device (BYOD) has become the growing trend in the business world. Instead of the company providing the necessary hardware/software for its employees' business operations, by approving BYOD policies, individual employees can choose their own devices to use at work (Zielinski 2012). According to a CISCO survey (Cisco 2012) of 600 IT leaders, 95% of companies responded that they already permit some form of BYOD in their organisation, and that by 2014 the average number of connected devices per knowledge worker will increase 18% to 3.3 devices per worker. There are many reasons for the large growth in allowing employees to use their own devices. One of the main benefits of adopting this kind of policy is productivity (Mont 2012). Research carried out on behalf of Dell and Intel last year (TNS Global Research 2013) concluded with that by allowing employees choose their own technology, had lead to increased workforce productivity because employees feel more comfortable using their own devices in the work place. It combines the possibilities of staying connected with their personal lives while at work, and also being available for work related issues while not at the traditional office setting. The variety of devices available and the amount of data they are capable of transferring, with the introduction of 3G and now 4G networks, is exponentially greater now than it has ever been (Cisco 2012).

With this increase of different devices, as well as the different operating systems being used, it has led to an amplified risk of exposure to viruses, malware and a host of other security issues, as well as the potential leaking of sensitive material and data (Morrow 2012). The difficulty lies in providing what the employee wants, along with the safety and security of the organisation's data. The employee would like to be able to use any device they want, whatever the operating system they choose and connect to the organisations network, and to be able to freely change the device should they wish to with no problem in its connection, whereas the organisation wants to ensure it has the safest policies in place to prevent any damage from happening, either intentionally or by accident (Thomson 2012; Keyes 2013).

The tendency over the previous years had been to implement a BYOD policy using devices from Blackberry as they were considered to be inherently safer, having a closed operating system and

with a focus on business consumers (Zielinski 2012; Keyes 2013). Following on from that were Apple and its range of products using the iOS operating system. In recent years the Android operating system has come to the fore of the mobile devices industry, thanks to the Google operating system being an open source system, and companies like Samsung, HTC and Motorola bringing out a range of new smart phones and tablets, and aggressively targeting businesses around the world (Harris & Patten 2014)

1.2 BYOD IN RELATION TO SME'S

According to the European Commission there are more than 20 million Small and Medium sized (SME's) in operation within the EU which represents 99% of all European businesses (European Commission 2014). This means that they are considered a key driver for economic growth, innovation, employment and social integration throughout the EU, and thus play a very important part of the economy. SME's are starting to see the benefits of adopting a policy of BYOD. Employees are considered happier and more productive when they are allowed to use their own devices, so it is only normal that SME's try to capitalize on this phenomenon. There is also the increased productivity potential by allowing employees to use their devices outside of normal business hours to get work done (Mont 2012). In a survey conducted by Nasstar in the UK regarding BYOD in SME's, 58% of responding companies reported that by allowing their employees to use their own devices at work had led to increased output and better workplace efficiency and happier staff (Nasstar 2012).

1.3 PROBLEM DESCRIPTION

According to Thomson (2012), who summarizes the Cisco "*Connected World Technology Report*"(Cisco 2011), many new younger employees have expressed a need to be able to work with their own personal mobile devices and expect to be able to use them within the confines of the enterprises network. They consider the security of these devices to be the responsibility of the IT department. They want to be able to work wherever and whenever they want, and expect to be able to do this securely. In an article by Morrow (2012), he suggests that BYOD seems likely to continue to rise and that the best companies can do is to seek solutions to address the problems and risks created by adopting this trend. Employees expect, according to Thomson (2012), user-support for their devices within companies, and to not accommodate the employees on this would mean decreased productivity, unnecessary risks, and could see the company labelled

as out of touch with the modern world, which could damage the company, especially from a recruitment perspective. Gammage (2010) predicts that 90% of organisations will support their enterprise applications accessed by employees' privately own devices by 2014, thus growing the need to support these with stronger services. Gammage (2010) also discloses that the underlying driver for this are the employees, who prefer to use their own mobile devices above the company's ones which are often seen as limited and outdated. However, smaller businesses can be considered to be more at risk because they are less likely to have the knowledge and resources to cope with the influx of employees devices on their systems (Harris & Patten 2014).

Consequently, there is a need for conducting a systematic literature review in this area that summarizes the existing knowledge about BYOD. The results of this study can assist organisations and researchers by providing them with useful information about BYOD and the issues involved with implementing it.

The main objective of this thesis is to summarize existing research on BYOD in relation to SME's, and identify any gaps that there may be, in order to suggest areas for further research. This thesis used a systematic literature review to identify and evaluate the current research.

This aim of the research is to address not only the risks professionals in the IT industry face as it looks to allow corporate data to be accessed from privately owned devices, but to also look at the opportunities that emerge from this. While BYOD can certainly offer a number of benefits to SME's, it also has to be managed very carefully as it brings about many new challenges. The make-up of a SME usually means there is not an established security department within the company, which can lead to oversights when allowing employees own devices to connect to the company's network.

This research will also outline the threats, risks and vulnerabilities associated with the use of an employee's own device such as smart phones and tablets within a SME environment, and also propose some solutions that can be adapted to company's policies to ensure the safety of the company's data.

1.4 Research Question

Considering the importance that BYOD is going to play in the near future, and the unlimited opportunities that personal devices and cloud computing technologies are going to open up for new and existing firms, it is clear that SME's will continue allowing for employees to use their own devices for business work. The main drawback, however, for SME's is the lack of robust security policies that will help to assist the firm's safe operation. The importance of being aware of the threats related to the adoption of BYOD and the establishing secure policies to deal with this is more evident than ever.

As a result, the main objective of this research is:

To understand how SME's can integrate a BYOD policy into their systems and be able to manage them securely.

To achieve this objective more effectively, we can extend it under the following sub questions.

SQ1. ***What risks and opportunities do professionals in the IT industry face with BYOD in a business environment?***

SQ2. ***What are the current common policies in regard to BYOD adoption?***

SQ3. ***What is the current state of BYOD adoption by SMEs?***

SQ4. ***What solutions can be provided to assist the aforementioned IT professionals in SMEs?***

1.5 Chapter Organisation

The research will be organized into five main chapters:

This thesis will follow the description of the systematic review which is conducted on academic and professional journal papers published from 2009-2014. The structure of the thesis is as follows:

- The first chapter gives a brief background to BYOD,describes the problem statement, shows the objective of the study, explains the importance of the study,and the present the organisation of the thesis.

- Chapter 2 describes the research methodology, giving a brief background to systematic review methodology and related work, and expresses the limitations of the research.
- Chapter 3 includes the results and analysis of the systematic review.
- Chapter 4 discusses the findings of the systematic review.
- Finally, the conclusion of the systematic review, accompanied with suggestions for future work is covered in Chapter 5.

2 Research Methodology

Okoli and Schabram (2010) identify three types of literature reviews. The first and most common type is the 'theoretical background' which is part of a journal article and helps give foundation and context to the research question. The second type is a "thesis literature review" which usually forms a chapter of a graduate thesis. The third one they identified is a stand-alone review paper which does not collect or analyze any primary data. This is known as a Systematic Literature Review (SLR) and shall be the basis of this paper.

A Systematic Literature Review (also sometimes referred to as a systematic review) is a form of secondary study that uses a precise methodology to identify, evaluate and interpret all available previous research related to a specific question in a way that is impartial and can be replicate(Kitchenham 2004).

2.1 Reasons for adopting Systematic Literature Review

Systematic literature reviews are carried out in accordance with a predefined search strategy, which must allow the completeness of the search to be assessed. There are numerous reasons for performing a systematic literature review. The most common reasons described by Kitchenham (2004) are:

- To review the existing evidence relating to a particular phenomena.
- To identify any gaps in current research in order to suggest areas for the further investigation.
- To provide a framework for arranging new research activities on the topic.

According to the advantages of a systematic review described by Kitchenham (2004), systematic reviews can be an efficient process to allow a researcher to get the information about the effects of a phenomenon across a wide range of settings and empirical methods, where it is less likely the results are biased.

The process this literature review follows are the guidelines which have been set out by Okoli & Schabram (2010). These guidelines recommend an eight-step literature review process that is academically thorough, complete and reproducible.

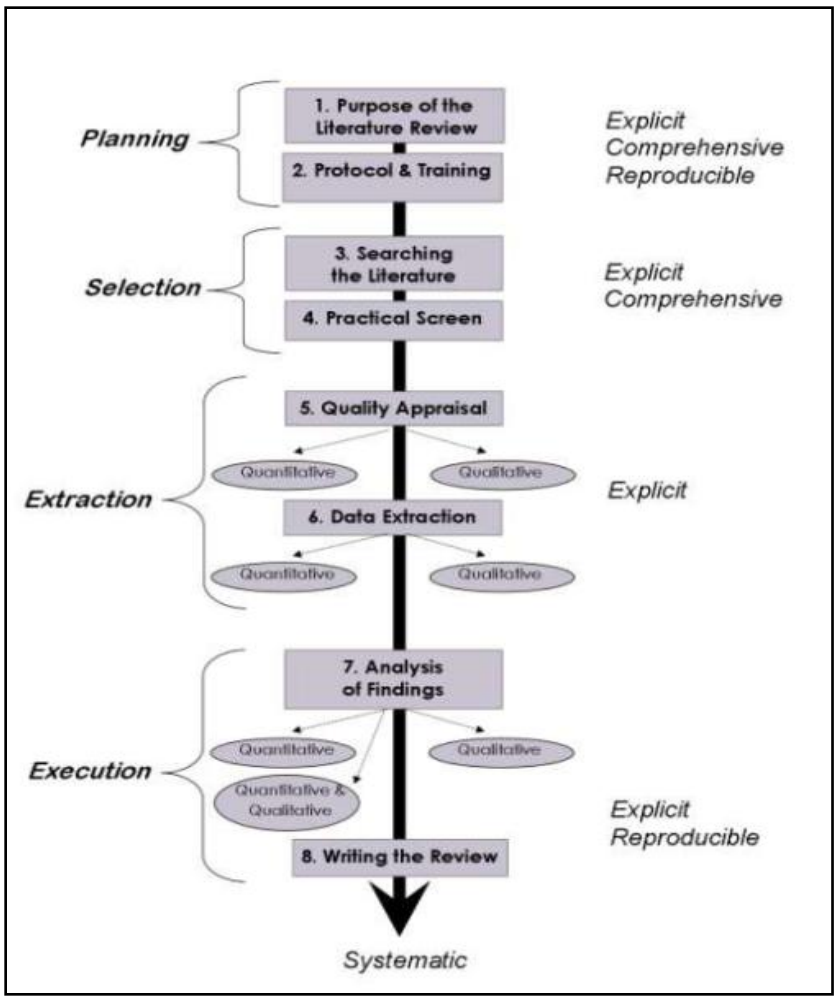

Figure 1: A systematic guide to literature review development (Okoli & Schabram 2010)

Step	Title
1	Purpose of the literature review
2	Protocol and Training
3	Searching for the Literature
4	Practical Screen
5	Quality Appraisal
6	Data extraction
7	Synthesis of studies
8	Writing the review

Table 1: Steps for a systematic literature review (Okoli & Schabram 2010)

2.2 Systematic Literature Review Protocol

Step one has already been completed and laid out in the introduction where it described the benefits of conducting a systematic literature review. The second step covers the protocol and training needed to conduct the review.

According to Okoli & Schabram (2010), this is among one of the most important stages of development. Here a plan is developed which will decribe the conduct of the review, which included the drafting of the research question, followed by the training of the reviewer. As this review is being conducted by only one reseacher, the training is considered not necessary as the protocol that has been laid out is being followed and therefore does not have to be learned.

2.3 Searching for the Literature

The search for literature for selection involved both searching for studies that would be included in the main body of my own study, and eliminating others which were found not meet the requirements. A broad scope was adopted at the beginning with searching for any articles, conference, or academic papers related to BYOD from a business perspective. It was then narrowed to BYOD research in relation to SME's.

A search for professional literature regarding BYOD policies was also carried out.

2.4 Literature search

The review was conducted by searching the databases available through Luleå University of Technology Library. An extensive search was carried out on the library database to find articles and journals that were relevant. By using a proxy offered by Luleå University Library, the same search terms were carried out on other research databases, namely ProQuest, Scopus, Web of Science, EbscoHost, IEEE Explore and Google Scholar. Using these databases, the articles and journals found were from peer-reviewed journals to give more credibility to the piece.

Using key-word Boolean searches, a large number of artides and journals were gathered together to be reviewed in more detail. Some other articles were also identified by referring to the references of the papers initially found through the searches. Finally, using Google Scholar, each article was checked to see if it had been cited in other works, and these new articles were then alsochecked to see if they were relevant for this review.

Once it became clear that no new articles were identified, the search moved forward to the 'practical screen' stage.

2.5 Results of the Literature Search

The term "Bring your own Device" is a relatively new term, and as a result the number of articles returned in searches was quite low. However this meant that many of the articles could be considered relevant as they were, paying particular attention to the advantages and disadvantages, considerations and other such topics such as implantation difficulties.

To give an example of the number of result returned, searches for the following keywords through different databases are laid out below:

Search name	Google Scholar	ProQuest	Scopus	Web of Science	EbscoHost	IEEE Explore
BYOD	5,890	13,583	104	9	1,247	35
Bring your own device	551,000	193,160	81	7	982	123
BYOD security	1,700	9155	56	3	139	23
Bring your own device security	257,000	88,158	50	3	61	34
BYOD policy	1,420	5,233	29	2	218	10
Bring your own device policy	334,000	75,859	24	2	512	11

Table 2: Initial search results

To make the results more relevant the timescale of the search was narrowed to 2009 – 2014. The reason for this is that "Bring your own Device" is a relatively a new concept and by doing this it was intended to filter out unnecessary results. Where the option was available, the results were limited to peer-review journals. The results of narrowing the search follow:

Search name + (2009 – 2014)	Google Scholar	ProQuest	Scopus	Web of Science	EbscoHost	IEEE Explore
BYOD	3,670	97	104	9	70	35
Bring your own device	48,700	8,043	81	7	73	77
BYOD security	1,550	53	56	3	7	23
Bring your own device security	23,900	2,488	50	3	1	29
BYOD policy	1,240	56	29	2	20	10
Bring your own device policy	28,300	4,250	24	2	49	9

Table 3: Key words search results from 2009 - 2014

Interestingly, even with the filters applied the results from both *Scopus* and *Web of Science* return the same as before.

However, when dealing with Small and Medium Enterprises specifically there was considerably less material available for review. To the above searched terms were added 'SME' and 'Small Medium Enterprise'. The filters of 2009 -2014 and peer reviewed were also left in. Below is the table of results;

Search name + (2009 – 2014)	Google Scholar	ProQuest	Scopus	Web of Science	EbscoHost	IEEE Explore
BYOD + SME	104	5	0	0	0	0
Bring your own device + SME	8,100	207	0	0	61	8,423
BYOD security + SME	66	5	0	0	36*	116
Bring your own device security + SME	23,900	79	0	0	119	730

BYOD + small medium enterprise	12,500	22	0	0	88	15,969
Bring your own device + small medium enterprise	16,200	1,144	0	0	2,045*	240
BYOD security + small medium enterprise	361	20	0	0	13	2,880
Bring your own device security + small medium enterprise	16,900	563	0	0	2,540*	59
BYOD policy + SME	90	4	0	0	39	132
BYOD policy + small medium enterprise	292	852	0	0	2,678*	43
Bring your own device policy + SME	6,650	70	0	0	297*	320
Bring your own device policy + small medium enterprise	17,100	852	0	0	2,678*	43
SME	56,100	10,842	4,096	1,486	5,410	1,404
Small medium enterprise	54,000	43,395	6,416	1,853	4,978	2,355
SME security	16,400	1,656	97	12	9	93
SME mobile security	11,500	278	5	0	1	9
Small medium enterprise security	28,300	13,146	239	0	6	208
Small medium enterprise mobile security	16,500	2,441	19	1	1	12

Table 4: Extended key word search 2009 - 2014

*__Note: The initial search query did not yield any results.__ However, using EbscoHosts 'SmartText Searching', results were found based on the keywords.

These search terms were used in the databases mentioned above, and although many of the searches returned generally the same articles, by using all the databases available the greatest possible number of results was returned.

During each of the searches, a number of articles were examined looking at the abstract, conclusion and keywords to see if they were relevant to the research.

In total 73 documents were put forward to the screening stage. 50 were related to BYOD and 23 dealt with SME's**. Only three were directly related to BYOD in SME's.

** It should be noted that 7 papers which were put forward for BYOD screening were also put forward for SME screening as their content covered both.

PROBLEMS WITH THE SEARCHES

While most of the searches were considered somewhat relevant to the topic, some irrelevant material did appear in the search. For example the acronym BYOD turned up some results related to the authors whose surname was 'Boyd'.

The search for SME returned a number of results related to an author named Sayed Mohammad Ebrahim Sahraeian and because of this, articles were very difficult to find using this search term.

2.6 PRACTICAL SCREENING

The articles that were found were sent forward for screening at the next stage. According to Okoli & Schabram, this is the stage where the researcher is explicit about which studies are for review and which studies should be discarded (Okoli & Schabram 2010).

2.6.1BYOD RELATED LITERATURE SCREENING

Of the 50 articles& papers which had been found it was necessary then to explicitly examine these to see which ones should be put forward to the next stage.

The criteria used to narrow down the search further were based on 3 questions:

No.	Question
1	Is the study related to the advantages & disadvantages of BYOD?
2	Is the study related to the implementation of BYOD?
3	Is the study related BYOD policies?

Table 5: BYOD screening criteria

By using these questions it was possible to further screen out a further 23 papers. This left 27 papers to be included in the quality appraisal.

2.6.2 SME RELATED LITERATURE SCREENING

Of the 26 academic articles which had been found it was necessary then to explicitly examine these to see which ones should be put forward to the next stage.

The criteria used to narrow down the search further were based on 3 questions:

No.	Question
1	Is the study related to the implementation of BYOD in a SME environment?
2	Is the study related to the implementation of BYOD in general?
3	Is the study related BYOD policies?

Table 6: SME screening criteria

By using these questions it was possible to further screen out a further 8 papers. This left 18 papers to include in the quality appraisal.

2.7 QUALITY APPRAISAL

The quality appraisal stage is when the researcher must explicitly set out the criteria which will be used to judge the articles and papers which have been sent forward to this stage in order to find the ones which shall be used in the final review (Okoli & Schabram 2010)

2.7.1BYOD RELATED LITERATURE QUALITY APPRAISAL

After the screening stage, a total of 27 papers were sent to the quality appraisal stage. Here each paper was read and examined to see whether it should be included for the final literature review report. The following criteria were used to appraise the quality of the remaining papers.

No.	Criteria Description
1	Methodology of research
2	Related to advantages and disadvantages of BYOD
3	Related to BYOD policies

Table 7: BYOD quality appraisal criteria

Below is the quality appraisal of the 27 papers using the criteria set out above:

Title	Author &Year	Purpose (context/comments/ methodology)	Advan. /Disadvan	Policies	Included (Y/N)
A survey of trust and risk metrics for a BYOD mobile worker world	Seigneur & Kolndorfer (2013)	A survey which establishes employees knowledge of risks	Y	N	Y
Acceptance of BYOD among employees at small to medium-sized organisations	Hensema (2013)	A paper about BYOD acceptance with Employees	Y	N	Y
Analyzing consumerization - Should enterprise business context determines ses- sion policy?	Copeland & Crespi(2012)	A conceptual paper looking at consumerization in the work place	Y	Y	Y
BYOD - Bring your own Device	Disterer & Leiner(2013)	A case study looking at the use of 'duel use' devices	Y	N	Y
BYOD Genie is out of the	Singh	A survey about the risks	Y	N	Y

bottle –"Devil or Angel"	(2012)	to data security			
BYOD usage by post-graduate students of the International Islamic University Malaysia: An analysis	Hamza & Noordin (2013)	A study of BYOD on a university campus	N	N	N
BYOD: An examination of bring your own device in business	Rose (2013)	A conceptual look at legal issues associated with BYOD	N	Y	Y
BYOD issues and strategies in organisations	Astani, Ready & Tessema (2013)	A case study about organisational strategies in coping with BYOD	Y	Y	Y
Changing user attitudes to security in bring your own device (BYOD) & the cloud	Lennon (2012)	A conceptual paper looking business user's attitudes towards utilizing their own devices for business.	N	Y	Y
Controlling enterprise context-based session policy and mapping it to mobile broadband policy rules	Copeland & Crespi (2012)	A design of method about controlling session policies for BYOD	N	Y	Y
Cloud service portal for mobile device management	Liu, Moulic & Shea (2010)	A design of method for a portal to provide remote management access for device management	N	Y	Y
Human resource issues in BYOD policy development	Ready, Astani, Tessema (2014)	A case study looking at creating a BYOD policy from a HR perspective	N	Y	Y
Implement network	Al Harthy &	A research paper	N	N	N

security control solutions in BYOD environment	Shawkat (2013)	looking at increasing network security for BYOD			
International data privacy legislation review: A guide for BYOD policies	Absalom (2012)	An industrial report for a guide for BYOD Policies	Y	Y	Y
Managing and securing business networks in the smart phone era	Mahesh & Hooter (2013)	A literature review of corporate policies and research papers	N	Y	Y
Managing mobile devices in hospitals: A literature review of BYOD policies and usage	Moyer (2013)	A literature review of BYOD policies in hospitals	N	Y	Y
Mobile device security considerations for small and medium-sized enterprise business mobility	Harris & Patten (2014)	A conceptual paper on security plans for SMEs	Y	Y	Y
New security perspectives around BYOD	Scarfò (2012)	A survey about the methods from the security point of view.	Y	Y	Y
Preserving privacy and accountability for personal devices	Gheorghe & Neuhaus (2013)	A conceptual paper on having policies for personal devices	N	Y	Y
Risk management in the era of BYOD: The quintet of technology adoption, controls, liabilities, user perception, and user Behaviour	Yang et al. (2013)	Design of model of understanding the BYOD practice and its relationships	Y	Y	Y
Security and risk consid-	PriceWaterHouse	Industrial report on the	Y	N	Y

erations for your mobile device	Cooper (2013)	risks associated with mobile devices			
T -dominance : Prioritized defence deployment for BYOD security	Peng et al. (2013)	Security protocols for BYOD	Y	N	N
The mobile execution environment: A secure and non-intrusive approach to implement a bring your own device policy for laptops	James & Griffiths (2012)	A conceptual look at BYOD policies for laptops.	Y	Y	Y
The risks of using portable devices	Walters & US-CERT (2012)	Industrial report from the USA government agency on the risks associated with portable devices	Y	Y	Y
WI-FI internet browsing architecture via BYOD for smart campus	Sangani et al (2013)	BYOD issues related to universities	N	Y	N
Wireless networks: De-velopments, threats and countermeasures	Noor & Hassan (2013)	Conceptual paper discussing threats in wireless networks	Y	N	Y
2TAC: Distributed access control architecture for "Bring your own Device" security	Chung et al (2012)	Design of method which uses double layer access control	N	Y	Y

Table 8: BYOD related papers

After the quality appraisal was completed, 23 papers and articles related to BYOD were put forward for the final literature review.

2.7.2 SME RELATED LITERATURE QUALITY APPRAISAL

After the screening stage, a total of 18 papers were sent to the quality appraisal stage. Here each paper was read and examined to see whether it should be included for the final literature review report. The following criteria were used to appraise the remaining papers.

No.	Criteria Description
1	Methodology of research
2	BYOD or device management in SME
3	SME security

Table 9: SME quality appraisal criteria

Below is the quality appraisal of the 18 papers using the above criteria:

Title	Year& Author	Purpose (context/comments)	Device	mgmt.	Security	Included (Y/N)
'Risky business': Perceptions of e-business risk by UK small and medium sized enterprises	Grant et.al (2014)	A survey on the risks with technology in SME's	Y		Y	Y
A survey of security risks of mobile social media through blog mining and an extensive literature search	W. He (2013)	Research looking at the risks associated with social media in the work place	N		Y	N
Acceptance of BYOD among employees at small to medium sized organisations	Hensema (2013)	Acceptance of BYOD among employees at SMEs	Y		Y	Y
Complete network security protection for SME's within limited resources.	Todd & Rahman (2013)	Report on how to secure a SME network	N		Y	Y
Cyber security scenarios and control for small and medium en-	Sangani & Vijayakumar	Security controls related to SME's	Y		Y	Y

terprises.	(2012)				
Drivers , benefits and challenges of ICT adoption by SME's	Barba-Sánchez et. al (2009)	A literature review on ICT adaptation in SMEs	Y	N	Y
Enabling open innovation in small- and medium-sized enterprises: How to find alternative applications for your technologies	Bianchi et al (2010)	Paper on the different applications available to help SME's	N	N	N
Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME	Kaur & Mustafa (2013)	A case study looking at security awareness of SME's	N	Y	Y
Mobile device security considerations for small- and medium-sized enterprise business mobility	Harris & Patten (2014)	A conceptual paper examining the security considerations for SME's	Y	Y	Y
Mobile technology - Enhanced asset maintenance in an SME	Bankosz & Kerins (2014)	A conceptual paper looking at technology and SMEs	N	Y	Y
Research on third-party E-business model of small-and-medium enterprises	Q. Hu (2011)	Business models of SME's	N	N	N
Rethinking IT governance for SMEs	Devos et. al. (2012)	A paper on the foundations of IT governance in SMEs.	Y	N	Y
Security risks in teleworking : A review and analysis	Yang et al (2012)	Literature review of the risks in telemarketing	N	N	N

Small business : Cyber security survey	Prince & King (2012)	A survey on the security risks facing SMEs	Y	Y	Y
Teaching cyber security: Protecting the business	Murphy & Murphy (2013	Conceptual paper on the perspective of cyber-security and the need for educational programs	Y	Y	Y
The risk and prevention of SME E-commerce operation***	Luoguifa (2011)	E-commerce risks for SMEs	N	N	Y
The usage and adoption of cloud computing by small and medium businesses	Gupta et al (2013)	Research paper on cloud security in relation to SME's	N	Y	Y
WI-FI internet browsing architecture via BYOD for smart campus	Sangani et al (2013)	Design of a system for Wi-Fi usage with BYOD	Y	N	Y

Table 10: SME related papers

After the quality appraisal was completed, 13 papers related to SME's and their securities were put forward for the final literature review.

*** The paper "*The Risk and Preventionof SME E-Commerce Operation"* had originally been accepted for the next phase, but upon the rechecking of the papers it had been found that it had since been retracted by IEEE and so has not been referred to in the analysis.

2.8 Data Extraction

After all the documents have been identified and gathered for inclusion in the literature review the next stage is to collect all the data from each study (Okoli & Schabram 2010). Each paper was reviewed again to ensure that it was valid for inclusion in the literature review.

2.9 Data Analysis & Synthesis

A total of 36 studies on bring your own device and small & medium sized enterprises were identified, and these covered many different study areas, such as conceptual study, industry experience report, case study, survey, and professional studies. Each study was reviewed by analyzing the context of the study, research questions, and empirical confirmation of the result. The studies covered a range of research topics within the BYOD phenomena and were conducted with a multitude of research methods.

15 studies (42%) were classified as conceptual studies which was the highest among the categories. There were 4 case studies and 5 surveys. A total of 4 papers were classified as industrial/ technical reports dealing with BYOD implementation and creating policies to secure it. 3 papers were literature reviews and 5 were papers where a new design of method or system was put forward. 16 out of the 36 studies were conference papers and the remaining 20 studies were published in journals. Figure 2 show the classification of studies that were reviewed

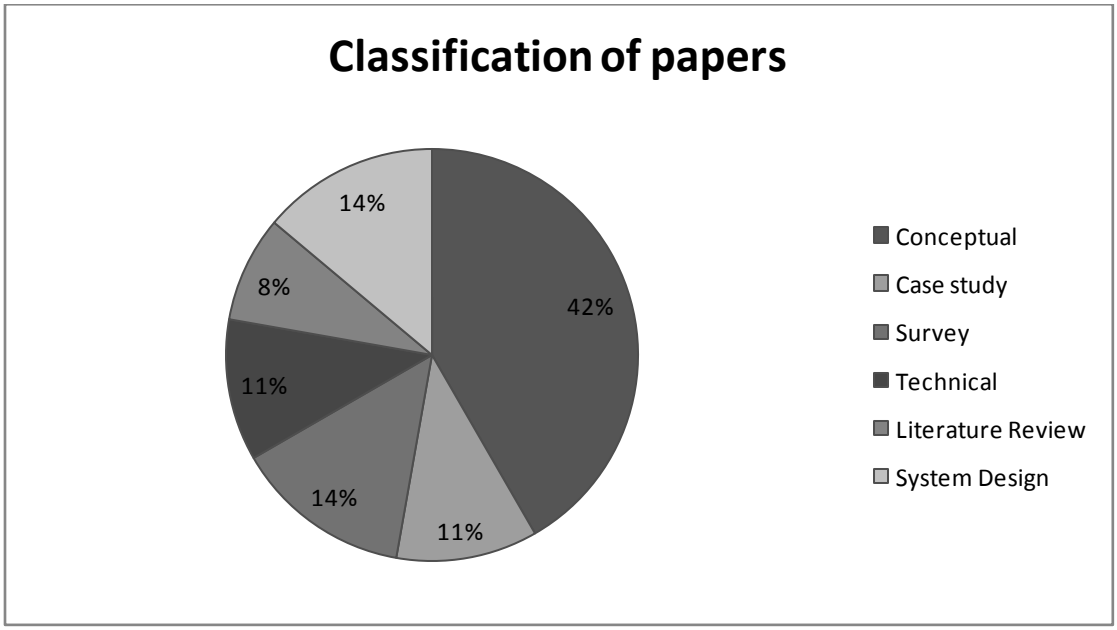

Figure 2:Classification of papers reviewed

Figure 3 shows that over the last 6 years (2009 – 2014) there has been an increase in the number of published papers covering Bring your Own Device and its place in the workplace. This is

not a surprise as it is a recent phenomenon. Figure 3 shows the breakdown of the years of the papers used in this literature review.

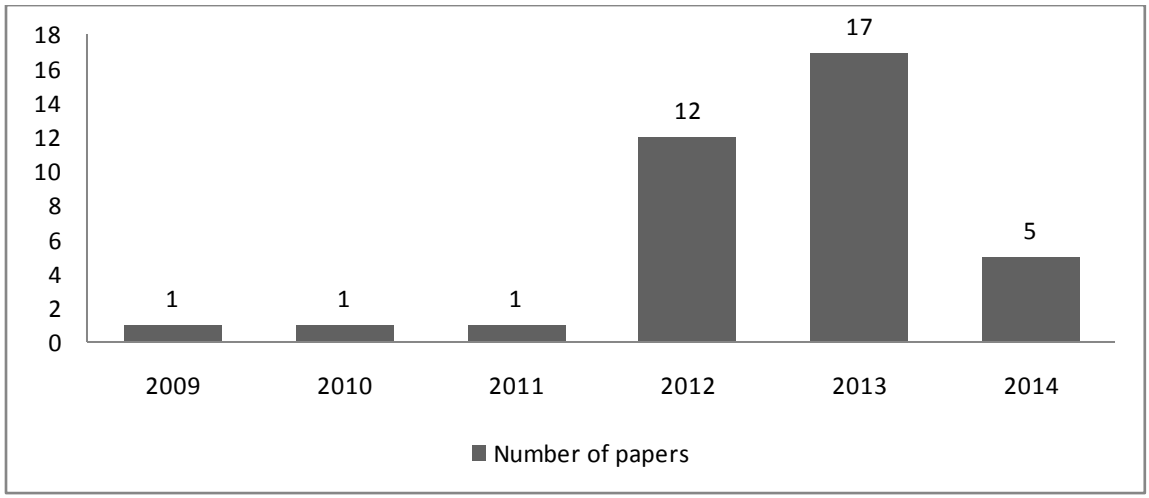

Figure 3: Number of papers included in the review from 2009 -2014

After collecting all the relevant data, and going through the screening process as part of a systematic literature review, the process then moved on to analysing the literature in order to be able to present the findings.

The data which has been extracted was synthesized so that it was able to answer the research questions which had been laid out in section 1.4. According to Kitchenham (2004), data synthesis can be either qualitative synthesis or quantitative synthesis. However, Kitchenham (2004) also states that descriptive (qualitative) analysis can be complemented with quantitative summary of data in order to enhance relevance in the decision making process.

Qualitative synthesis consists of the extracted information, such as that of population, context, sample sizes, or outcomes, etc. being presented in a consistent scheme according to research questions. The presented tables should be arranged to highlight any similarities or differences between the study outcomes. It is also important to recognize if the results are consistent or inconsistent with each other. Some methods used in qualitative synthesis include meta-ethnography, meta-study and meta-synthesis (Kitchenham 2004; Cooper et al. 2009).

Quantitative synthesis involves taking the results from the different studies and presenting them in a format which includes sample size of intervention, estimated effect size for each intervention, and the differences between the mean values for each intervention. Meta-analysis is often used to find the statistical significance of these findings (Kitchenham 2004; Cooper et al. 2009).

According to Silva (Silva et al. 2013), human aspects of interest are often better understood using qualitative research as they offer insight into social, emotional and experimental phenomena, and as such is used in this thesis to analyse the phenomenon ofBYOD. Interpretive or qualitative approaches are the preferred research strategies when "how" and "why" research questions are being asked (Merriam 2009).

There are many methods for carrying out qualitative synthesis, such as meta-narrative synthesis, critical interpretive synthesis, meta-study, meta-ethnography, grounded formal theory, thematic synthesis, textual narrative synthesis, framework synthesis and ecological triangulation (Barnett-Page & Thomas 2009). Following a review of these, it was decided that thematic synthesis would be used for data synthesis in this thesis.

Thematic synthesis was developed by Thomas and Harden (Thomas & Harden 2008) as an approach to synthesis which combines and adapts approaches from both meta-ethnography and grounded theory (Barnett-Page & Thomas 2009). Its use in systematic reviews is to bring together and integrate the findings of multiple qualitative studies into one study. Thematic synthesis is a technique for identifying, analyzing, and reporting patterns or themes within data (Cruzes & Dybå 2011).

Thematic synthesis was found to be the most suitable method for this thesis, making it possible to be more critical about the area of interest with the purpose of producing a practical model for using BYOD within an organisation and for also assisting in the creation of BYOD policies in SMEs.

Thomas and Harden (Thomas & Harden 2008) created a method which had 3 stages to it; which were to code the text, develop descriptive themes, and then to create analytical themes. These stages were originally created to work on health issues research. Cruzes and Dybå proposed the following method to carry out the synthesis stage (Cruzes & Dybå 2011) in software engineering

research, and as such it forms the basis of synthesis in this research. Their proposal contained 5 steps.

2.9.1 PRIMARY DETAILS EXTRACTION

The first step was to read all the texts thoroughly, to allow the reader to get immersed with the data. Doing this allows the author to become more familiar with the comprehension of the information. Having become familiar with the literature, the objective then was to extract data from the primary studies, which included bibliographical information,the aims, context, and the results of the studies. The technique used to extract the data was proposed by Cruzes et al, (Cruzes et al. 2007) in which they provided a template to assist with the data extraction. Cruzes and Dybå (2011) suggested that there are three kinds of data that can be extracted:

- Publication details (authors, year, title, abstract, etc.)
- Context descriptions (subjects, technologies, etc.)
- Findings (results, actions,phenomena, events, etc.)

Table 4 shows an example of the template used during the extraction phase. The headings used are from the previous papers mentioned (Cruzes & Dybå 2011; Cruzes et al. 2007).

Title	New security perspectives around BYOD
Type of study	Survey
Author (s)	Antonio Scarfò
Year	2012
Goals	To show the emerging methods and models to approach the BYOD phenomenon from the security point of view
Subjects	Security professionals working in enterprise organizations
Results	A hands-off approach is key to workers productivity, and to achieve this MDM should be implemented

Actions	BYOD should be simple and friendly as possible, leaving the necessary constraints to be enforced just in presence of critical situations

Table 11: Data extraction template

When relevant data was found in the literature it was highlighted and a note was made. As there was only one researcher, this process was quite slow as the extracted information has to be revised again. Ideally there would have been a second researcher to check over the extracted information.

For this section, Mendeley® reference managing software was used to record the data from each paper.

2.9.2 CODING THE DATA

The next step was to code the data. This involved trying to identify any interesting concepts, categories, findings or results, and to then try to find connections between these codes and all the texts. A deductive approach was used to code the data. It starts with creating a tentative 'start list' of codes(Cruzes & Dybå 2011). This list was created using the research questions, the known problem areas, and theoretical concepts.

Thirty codes were used to create the 'start list'. The words used were created from the problem areas and theories found during the data extraction and also from the research questions. These codes were then attached to different portions of the text in an attempt categorize the many segments of the table. Table 12 shows the 'start list' of codes used to code the data

'Start list' of thematic codes

Advantages	Lost data	Trust	Value
Disadvantages	Finance	Authentication	Risk
Policies	Profiles	Integrity	Security
Solutions	Permissions	Confidentiality	Awareness

High risk	Social networks	Users	Convenience
Goals	Expectations	Devices	Conflict
Support	Professional	Formal	Informal
Ambiguity	Education		

Table 12: 'Start list' of thematic codes

As coding was a critical step in the process, it was important that it was completed with attention to detail. Using these codes, the literature was again review and highlighted to indicate the where the code was present.

2.9.3 Creating the themes

The third step moved on to translating the codes into themes. By creating themes, it helped to reduce the large amounts of codes into a smaller number of analytic units. To create themes, the codes created during the second phase were combined to make an overall theme. Themes pull together the codes into more meaningful units (Cruzes & Dybå 2011; Thomas & Harden 2008).

To begin with, the codes were grouped together using a mind mapping process. Doing this created what is called a thematic map. This helped to organize the codes to begin the process of translating them into themes. Similar codes where grouped together to try and create themes from them (Cruzes & Dybå 2011). An example of the process is shown in figure 4.

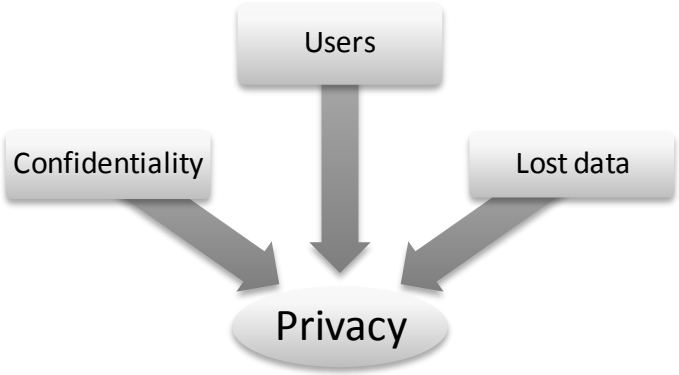

Figure 4: An example of the mind mapping process

When some of the codes overlapped into a second theme, the process was to go and adjust the original code so that they were only applicable to a single theme. This process also allowed for the creation of some more codes.

2.9.4 Modelling higher-order themes

The forth step involved trying to model higher-order themes by exploring the relationships between the themes created in the third step.The objective in this step was to combine some of the related themes in order to create a single, higher-order theme. The themes which emerged from the previous step were explored further in order to find relationships between them (Cruzes & Dybå 2011). This was done by referring back the now extended thematic map, which gave a clearer idea of the links that existed between the themes. Using the map, it was possible to group themes which had a clear relationship to each other together, and these themes combined created the higher-order themes.

The connection then between the higher-order themes and the central theme was then established.

2.9.5 Assessing the trustworthiness

The fifth and final step involved trying to assess the trustworthiness of the interpretations which lead up to the formation of the themes. This was done by making sure the research questions were answered based on the evidence of the thematic synthesis. The codes, themes and higher-

order themes were checked once again to ensure that no relevant data had been excluded, or any irrelevant data included.

The one negative aspect of this step was that it had been suggested that second researcher should also check the trustworthiness to ensure it is correct, but in this case it was not possible.

As mentioned previously, these steps were carried out using Mendeley® reference manager and Microsoft Excel® to organize all the research material so it was possible to code the data and create themes.

2.10 Limitations of the Literature review

This section addresses the limitations and validity threats to this systematic review.

Whilst this literature review sought to be as systematic and comprehensive as possible, there were some limitations. The research papers selected were English-language papers only; those in other languages were automatically discarded. As this systematic review was conducted by an individual researcher, there is the possibility that the validity could be questioned as opposed to if the thesis was conducted by several researchers. The reasons for this are that the articles selected on individual judgement and could be considered to be open to bias. These biases could have influenced the primary studies that were selected and also the data extraction phase, as well as its outcomes of the results. In effort to avoid these biases, every task has been carried out multiple times to try and ensure the results were accurate. An example of this involved rechecking the articles multiple times to ensure the references for them where accurate and true to reduce any mistakes by investigator.

The search for papers may be considered to create some limitations on the thesis. It was decided to use ProQuest, Scopus, Web of Science, EbscoHost, IEEE Explore and Google Scholar as the main sources of this systematic review. These databases are among the best known and most common databases used in similar systematic reviews. Another reason for choosing these databases was that Luleå Tekniska Universitet has been granted unlimited access to these databases. To reach the goal of finding as many relevant papers as possible, various search strings were used to cast the widest net possible to find the most relevant papers. After exploring the search strings in each database, the abstract was read of each paper that was on the first 2

pages of the results. The reasoning for this was that it was believed that the most relevant papers to the search strings would have been presented on the initial pages of the search.

The amount of material available on BYOD being used specifically in SMEs was also considerably smaller than originally anticipated. There were a lot of papers dealing with BYOD in general, how to implement them in businesses etc., but the vast majority of papers used in the cases of SMEs dealt with security issues they face and managing technology. While there were some papers found that dealt with BYOD, this should be considered an area for future work.

3 FINDINGS

This chapter will give a brief analysis on the main findings of this thesis using thematic synthesis. Using the themes found during the synthesis process the following chapter gives an insight into opportunities and risks that arise from adopting BYOD. The results given will help define some areas for which future primary and secondary research studies might be needed.

3.1BYOD RELATED LITERATURE

3.1.1 WHAT IS BYOD

BYOD is a business policy which is adopted by management to allow employees to use their own personal devices, such as tablets and smart phones. The employee is then allowed to use their own device for business operations instead of having to rely on business provided devices (Singh 2012).

Despite the fact that BYOD is a relatively new trend, more and more research is appearing all the time covering all aspects of the opportunities and threats associated with adopting such policies. This section of the report will look at those opportunities and threats and also some of the policies that are used in workplace.

3.1.2 BENEFITS OF BYOD

There are many perceived advantages and benefits for companies adopting BYOD policies. By embracing the use of personal devices for business purposes companies can gain many benefits. Managers have reported rising productivity and a willingness to work on projects after business hours as two of the main benefits being witnessed (Copeland & Crespi 2012a; R. Walters 2012). This added flexibility of using the same platform for both personal and business uses has enabled work to be completed more often out of normal business hours than ever seen before (James & Griffiths 2012). This has allowed an *"Anything, Anywhere, Anytime"* mentality to be created which has diminished the boundaries between private and professional life in regards to working hours (Disterer & Kleiner 2013).

There is also an increase in the collaboration among employees (Seigneur & Kölndorfer 2013). By using their own devices when collaborating on projects employees tend to use their device

more effectively (Scarfò 2012). Independence and competence among employees have also seen an increase and these can be considered to be advantageous (Hensema 2013).

There are many cost reductions that come with adopting BYOD in relation to hardware used in the business. Companies who offer BYOD generally offer an allowance for devices to be purchased. On many occasions an employee will supplement this to buy a more powerful device which leads to increased hardware capabilities in the business without having the extra cost (James & Griffiths 2012; Rose 2013).

There are also reductions in the cost incurred in the maintenance and upkeep of the devices and appliances. As the employees are now the owners of the devices, the cost associated with the upkeep have been transferred to them from the organisation (Singh 2012).

Singh also reports that it is now easier for users to switch to the latest versions of devices, meaning they don't have to wait for their employers to carry out an organisation wide update of devices (Singh 2012).

By having BYOD available to their employees, it can give an organisation a competitive advantage over others, by attracting the best pool of employees from the market. Having BYOD in the workplace helps to attract top grade employees because it assists with flexible working times (Hensema 2013; Singh 2012). In addition, Hensema (2013) talks about how "Generation Y" employees a driving force behind BYOD being adopted by companies. Generation Y are described as those who grew up with technology and expect to be able to use it both at home and at work (Hensema 2013, p.1).

As the employees are already familiar with the device, it can help to reduce the training time thereby increasing the productivity and efficiency of the employees (Ready et al. 2014). Overall BYOD offers financial benefits as well as other benefits that are much harder to measure such as a more productive workforce (James & Griffiths 2012).

3.1.3 BYOD Risks and Challenges

However, it is not all positive when adopting BYOD. Many of the devices used by employees in the workplace, such as iPads' and Android devices, were not designed primarily with exhaustive data security features in mind (Mahesh & Hooter 2013). This can leave to a weak point in the business security model which could lead to exploitation.

3.1.3.1 DATA LEAKS

One of the biggest risks associated with BYOD is that of data being leaked or lost. These losses can happen through a variety of reasons which will be covered below. When these losses happen they have a severe affect on the business, ranging from damage to reputation, financial penalties or a lawsuit (Moyer 2013). There is also the possibility that a competitor may gain access to the data and use it to gain an advantage over the business (Morrow 2012).

3.1.3.2 LOST DEVICES

A major threat to companies is data theft. Due to improvement in the storage capabilities over the past number of years, the amount of data that can be stored on device today is quite a considerable amount. Any accidental loss of a device could lead to a significant data breach (Mahesh & Hooter 2013). Even if a lost device does not contain confidential data, it could still be possible for criminals to use it to gain access to the enterprise network through the use of apps or cached information (Copeland & Crespi 2012a).

3.1.3.3 COSTS

According to Singh (2012) BYOD will bring cost reductions to hardware acquisition,it is possible for some additional costs and difficulties to be attributed to its implementation along with the cost of security. This is because the devices are more prone to theft and as such the valuable data stored on them needs to be protected (Singh 2012).

The environment used to transfer and store company data and applications must be encapsulated to make sure it is not exposed to risks when used on personal devices. Establishing this access to company data and applications and securing it is normally quite expensive (Disterer & Kleiner 2013; Seigneur & Kölndorfer 2013).

The costing of device usage could also lead to difficulties. If a device is used for both personal and business uses then this can lead to problems for the accounting department as it can be difficult to measure the cost correctly (Mahesh & Hooter 2013).

3.1.3.4 LOSS OF CONTROL

Many of the security problems associated with BYOD are a result of the lack of controls available to the IT department on the end users device, therefore there is also a lack of control over the company's data which has security implications for data leakage, data theft and regulatory obli-

gations (Morrow 2012). IT departments often have no physical control over the devices because of their mobile nature (P. Walters 2012). There is the risk of the device being stolen resulting in the loss of sensitive information, or the possibility that a person without the proper clearance may access stored and classified information. In fact it is stated that the most difficult part of BYOD is the actual enforcing of policies an organisation may have in relation to BOYD (Scarfò 2012).

3.1.3.5 APPLICATIONS

Applications (apps) can be used in the work place to help make an employee more productive. While some companies can afford to develop their own apps to be used, such as Intel, most companies rely on those from 3rd parties. Issues may arise when applications have to be used around a wide range of devices and operating systems, as not all applications may work on all versions (Rose 2013).

Apps for personal uses may also bring some problems. Apps have been known to contain vulnerabilities which may unintentionally expose the app to exploitation. A possible security bug in personal apps (social media, blogs, etc.) could be used to gain access to corporate information (Ernst & Young 2013). It is also necessary to ensure that employees know the dangers of downloading apps from outside the official repository for them (i.e. Google Play & iTunes). Apps for these 3rd party apps stores are significantly more at risk to malware infection due to the fact that the security controls aren't as strict as they would be from the official stores (Astani et al. 2013).

3.1.3.6 MALWARE

Another major concern is that of mobile malware. These can be installed on devices through applications downloaded and installed through public app stores. This can be considered to be a very pressing issue especially in relation to Android devices. As they are on an open platform, itmakes it much easier for developers to write malicious applications for it (Ready et al. 2014; Morrow 2012). This means that devices which unwittingly have malware installed on them, could be connected to the corporate network and inadvertently leak sensitive data (Morrow 2012). Malware is increasingly being written to collect information from devices, meaning that information stored in the cache, which is often stored in the clear, is being stolen. This information could include usernames and passwords being stolen (Morrow 2012)

There is also the threat of phishing were the user is tricked into using a fake website to access business accounts, which could also compromise the business systems integrity (Ghosh et al. 2013).

3.1.3.7 TECHNICAL SUPPORT

Fragmentation can be considered another problem for the security department to try and keep up with. According to Google (Google 2014b), fragmentation of the Android OS for April 2014 now stands at;

Android version	% in operation (?)
Froyo	1.1
Gingerbread	17.8
Honeycomb	0.1
Ice Cream Sandwich	14.3
Jelly Bean 4.1	34.4
Jelly Bean 4.2	18.1
Jelly Bean 4.3	8.9
Kit Kat 4.4	5.3

Table 11: Fragmentation of Android OS

This means there is a possibility for the security team having a range of devices on the network that have different security features. For example the new Android OS – KitKat, offers improved cryptographic algorithms which the older versions do not (Google 2014a).

It is not just the Android OS which caused problems. A recent update to Apple's iOS (version 7.1, released March 10th2014), fixed an important security hole involving SSL (Apple 2014). It would be important that all devices running the older version of the OS would be updated immediately as once the security issue was widely known, then the devices would be more vulnerable to attack. Having the device updates in the sole control of the employee means that not all devices might be updated immediately (Mahesh & Hooter 2013).

The IT security department will now have to manage and secure a wide range of devices including smart phones and tablets that use different operating systems, and potentially also different

OS versions, all accessing corporate data. It can also be challenging for the department to ensure that applications required for business operations that were running smoothly before an update, continue to do so after it (Rose 2013; Morrow 2012).

3.1.3.8 EMPLOYEES

There are many difficulties associated with an "*any device, anywhere policy*". Many employees would like to be able to have any device they want and not to be restricted in their choices. A policy like this could lead to unsuitable devices being introduced to the network (Scarfò 2012).

3.1.3.9 EMPLOYEE PRIVACY

If security is the main concern for the company, then privacy would be the major concern for the employee. Mobile devices may contain a lot of data which a user might consider private. Implementing any of the security measures on a personally owned device has a potential to affect an employee's right to privacy. Employees should be made aware of what exactly will be monitored or accessed on their devices. Employees should also have given explicated permission for the monitoring to take place. Without this there is a violation of the employees right to privacy (Absalom 2012; Gheorghe & Neuhaus 2013).

3.1.3.10 LEGAL

Before considering implementing a BYOD policy, an organisation must be aware of the legal implications of doing so. If an employee were to download an illegal file onto their own device during business operations, who would be liable for copyright infringement? It would be important for the company to ensure that employees comply with legal requirements regarding digital rights on BYOD devices, because it could be leave the firm legally responsible for employees' misconduct (Copeland & Crespi 2012a).

3.1.3.11 DATA PROTECTION

Customers of organisations have the right to have their data protected. In the event that a device is lost or stolen, this data has the potential to be leaked and as a result of this, there could be damage to the reputation of the organisation as well as legal costs to be covered (Mahesh & Hooter 2013).

In a BYOD environment, data protection does not only apply to corporate data, but also to personal data. In the EU, the Data Protection Regulation Act 2012 states that a person has the

"right to be forgotten", meaning that its personal data can be deleted without difficulty. In regard to BYOD, this means that companies must implement appropriate measures for the security of the data, and in the event of a breach the employee has the right to be notified (Ernst & Young 2013; Absalom 2012).

3.1.4BYOD Policies

The need for a well-defined policy governing the use of one's device in the workplace is essential for giving guidance to employees on what is expected of them when using their devices in work situations (Ready et al. 2014).

BYOD policies are needed to put constraints on employees wishing to partake in using their own devices. Some of these constraints include the use strong passwords, enabling file encryption to encrypt the data which is on the device, enabling automatic locking after a period of inactivity, managing the wireless network interfaces and the use of remote locking in the event of the device being stolen or lost (Hensema 2013; Ready et al. 2014).

The device should automatically be monitored, and if any violations are detected, they should be reported immediately (Ready et al. 2014). However, the monitoring of emails and voicemails has to be carefully regulated being mindful of data protection legislations. All monitoring must also be consented by the employee (Gheorghe & Neuhaus 2013) as it considered illegal and unethical to observe employees without their knowledge.Across different localities, data privacy legislationsspecifies that individuals must be fully informed and have given their explicit permission for their personal data to be accessed and processed(Absalom 2011).

Role-based access control should be implemented so that it is possible to limit what can be accessed. The system should have directory services integration which should be able to assign roles to users. Application-level filtering can be implemented using the latest generation of firewalls. Using this it is possible to know which applications employees are using and which sites they are trying to access. The network traffic should also flow through a device which can check for viruses or any malicious activity (Chung et al. 2012).

Copeland and Crespi (2012b) propose a policy titled "enterprise Business Context" (eBC) policy which enables the managing of business resources per request, and helping to manage employee spending while at the same time allowing employees full independence for personally

activities. The policy essentially groups tasks together into four context groups; Roles, Tasks, Factors, and Attributes. Each context will have been defined by the organisation according to job descriptions and as such will have credit limits and privileges regarding access to resources assigned to each context. For example, it is possible to set location factors such as 'at home' or 'at enterprise branch' which would determine what permissions would be granted to the user. In the case of the user being at home, they would have restricted access to the company's resources, and the data usage for that time period would be charged to the user. In the case of the location being based in the branch, then the restrictions would be lifted on the access, and the data usage charged by the carrier would be paid by the enterprise. It is also possible to apply the same rights and restrictions based on job title (executive, engineer, etc), tasks (working from home, working while travelling etc.) and other characteristics (Copeland & Crespi 2012b).

It is vital to restrict which applications may be installed through the white-listing or blacklisting of apps. The device should also always be kept up-to-date and this includes the applications installed on the device (Keyes 2013; Harris & Patten 2014).

It is also recommended to employ a virtual private network (VPN) or some other type of encrypted communication which would give limited access to the company's network for the communication between devices and servers (Disterer & Kleiner 2013). VPN's establish a secure, managed private tunnel between the user's device and the organisations IT networks. VPN's are usually implemented on the user's device by installing a VPN client app on it, and then having that app connect over a public network with a VPN gateway, which connects to the corporate network to keep all communications secure (Mahesh & Hooter 2013).

As well as having these policies in place, almost as important is having effective training in operation, to train the employees how to stay secure, and to be aware of the dangers of connecting to unsecure Wi-Fi networks (Astani et al. 2013) It is also important that users are able to find these policies to be able to review them (Lennon 2012).

3.1.5 Mobile Device Management

Appropriate security policy and procedures, training and awareness, network auditing and need access controls should all be considered as an integral part of any BYOD policy. To help ensure all these requirements are carried out, many organisations today adopt mobile device manage-

ment (MDM) software on their devices. Mobile Device Management represents a central point of administration of all devices being used at a company with regard to company policies (Disterer & Kleiner 2013). The MDM software will store all company-related data, such as calendars, emails and other applications in one area on the device and then ensure that the area is password-protected and secure (Astani et al. 2013). This can be includedon all BYOD devices and to secure all platforms and models of mobile devices at the same time within the same system (Harris & Patten 2014). This gives employees more freedom in choosing the device they would like to use without restrictions.

MDM systems are devised to provide many basic device management functions such as updating firmware, the installing or uninstalling of software, checking user preferences, and remote wiping of data from compromised devices. This system also ensures email, calendar and contacts in their system are consistent across the organisation (Liu et al. 2010). For many companies Mobile Device Managementis considered to be the ideal accompaniment to having BYOD (Disterer & Kleiner 2013).

3.2SME RELATED LITERATURE

Information technology and Information systems (IT/IS) play a very important role in the role of a modern Small & Medium Enterprise (SME). They can help reduce operating costs, or enhance their market capacities (Grant et al. 2014). However, due sometimes to their size or budget, they cannot always invest significantly in the area of information security (Murphy & Murphy 2013).

According to Murphy& Murphy (2013) the reason for lack of investment in security by SME's comes down to a couple of factors. There are limited finances for IT operations as a whole, a restricted amount of time that could be spent training the right personnel, and there is a lack of understanding of the risk of what could potentially happen. In a recent survey undertaken in association with Lancaster University in the UK (Prince & King 2012) it was reported that out of the 98 SME's surveyed, only 47% of these spend less than 5% of their budget on security. They also described that only 45% of these SMEs have ongoing security training, and a fifth of these companies, after the initial induction phase is completed they never train their employees again.

There is also a shortage of specialized security technicians available to SMEs to design and maintain the security architecture that is required (Sangani & Vijayakumar 2012). Due to the smaller nature of the business, many business decisions can be considered reactive and shorter-term, compared to larger company (Grant et al. 2014). According to Sangani and Vijayakumar (2012) many SMEs were not using the most common cyber security protection of implementing anti-virus programs because they did not perceive the attacks would happen to them. Security is generally an afterthought for most SME's until an actual cyber-attack happens to them (Sangani & Vijayakumar 2012)

Cyber security threats and weaknesses in information systems are the considered a major obstacle faced by SMEs without having the correct implementation of IT Security polices and a data protection mechanism (Sangani & Vijayakumar 2012). Viruses and worms, credit card fraud and denial of service attacks have been identified as the most frequent attacks that occur against SME's (Grant et al. 2014).SMEs cannot afford to either lose customers or decrease customer trust. It is important that SME's protect their customers information just as the larger enterprises do (Harris & Patten 2014), or they face the possibility of damaging their reputation (Prince & King 2012).

In 2012, PriceWaterhouse Coopers reported that 76% of small businesses in United Kingdom suffered a security breaches which caused some sort of financial loss (Kaur & Mustafa 2013). This kind of breach shows the importance of having stronger security controls in place in all SME's in order to prevent these breaches from occurring in the future.

Information security strategies and policies

As well as trying to keep existing systems secure, such as desktop computers, SME's and their IT professionals now also have to contend with making mobile devices secure. These new security concerns raise issues about the security of the enterprise's data and information. There is also concern about an employee's own personal information when they are using personal devices for business concerns (Harris & Patten 2014).

To deal with this, it is important that the company adopts a comprehensive device policy which should clarify acceptable use of mobile devices. It should deal with security measures such as limit network access to only authorised and verified users, transmitted data should always be encrypted, and remote wiping of devices should take place if sensitive business data has being compromised (Bankosz & Kerins 2014).

Currently in SMEs, the strategies and policies being implemented are said to be lacking. Again the reasoning for this is lack of funding (Devos et al. 2012). According to Devos, 54% of organisations are lacking sufficient plans that educate their staff about security risks. Companies cannot afford to employ in-house IT security personnel and as result are forced to subcontract information security services to external companies. Although outsourcing can be cost effective in managing information security it can have damaging consequences as confidential information can be compromised. According to Sangani and Vijayakumar (2012) many managers consider implementing IT Security means just installing an anti-virus program or employing a firewall, which continues misconception among SME's that cyber security issues are only consideration for larger organisations.

According to PriceWaterhouse Cooper research, only 63% of small businesses have a formally documented information security policies, which is a surprisingly low figure considering the information stored by the business could be a potential target for cyber theft (PriceWaterhouse Cooper 2012).

3.2.1 BYOD IN SME'S

During the literature search it became obvious that there has been a lack of research into the study of BYOD specifically in SMEs. One of the issues which was identifies for SMEs was that they must insure that there is a consistency between new BYOD policies they create, and any existing security and privacy policies that should already be in place (Navetta 2012a). Due to employee privacy concerns regarding information on personal devices, a standard device security policy which would normally contain information on the security and configuration of a device, would have to be amended toallow for access to non-company owned devices in the event of a security breach (Navetta 2012b).

4 DISCUSSION

Based upon the findings of the analysis, the following chapter gives a brief discussion on how the findings of the analysis can help answer the research questions.

To remind the reader, the mainobjective of this research is:

To understand how SME's can integrate a BYOD policy into their systems and be able to manage them securely.

To achieve the answers to this more effectively, the research question was then extended into the following sub questions:

SQ1. ***What risks and opportunities do professionals in the IT industry face with BYOD in a business environment?***

There has been much research into the opportunities and risks of having BYOD in the workplace. Among the main advantages or opportunities being witnessed in the workplace are a rise in productivity, and a willingness to work on projects after business hours. There is also an increase in the collaboration among employees as they feel more comfortable in using their own devices at work.

Another important benefit is the cost reduction being witnessed by companies, as they have less hardware to buy for business operations. This in turn can free up capital to be used in other areas. It has also been observed that employees generally buy a more powerful device which leads to increased hardware capabilities in the business without having the extra cost.

Being able to attract highly skilled employees as they consider workplaces that allow the use of BYOD as a much more attractive place to work is also considered an advantage.

According to Walters (R. Walters 2012) many employees already use personal devices and make use of cloud based applications, so it is important that companies take advantage of that situation.

However, there are also some drawbacks to allowing BYOD into the workplace. The main oneis that of data being leaked or lost. These losses can happen through a variety of reasons and when these losses happen they have a severe affect on the business, ranging from damage to

the reputation, financial penalties or even a lawsuit.Organisations need to be concerned about the state of the security on devices in use and the risks to which they may expose sensitive data to. Malware and cyber-attacks are continuing to be on an upward trend and have the potential for unauthorised access to valuable information (Morrow 2012).

Another major threat is that of data theft. Due the amount of data that can be stored on device today any accidental loss of a device could lead to a significant data breach.

There are many other such threats such as loss of control of the devices by the organisation which can have detrimental effects on the organisation, which are seen as the disadvantages of allowing employees to use their own device in the workplace. Enterprises have less control and visibility over unmanaged devices which mean there are fewer mitigation options available in the case of a lost or stolen device (Morrow 2012). Organizations cannot control the end user's choice of browser, version or when security patches are installed (Mont 2012) meaning that could potentially be leaving themselves exposed to a security breach.

Data protection is another big concern as customers of organisations have the right to have their data protected, while companies are also obligated by law to ensure this data is keep secure and protected from intrusion. In the case of companies wishing to monitor their employees' mobile devices as part of security measures, to do so lawfully, they must make sure the employees are aware the monitoring is taking place (Walker-Osborn et al. 2013).

It would also be important for the company to ensure that employees comply with legal requirements while using their devices, as any misconduct could be leave the organisation legally responsible and open to lawsuits.

SQ2. What are the current common policies in regard to BYOD adoption?

Writing a BYOD policy forces companies to think about what things the employees might be able to do on their own device while at work. When an organisation decides to allows employees own devices to be used within the confines of their network, then it is of the upmost importance that the policies they have in place cover the organisation from all possible angles.

BYOD policies are needed to put boundaries on employees wishing to use their own devices in the workplace. Among these constraints are the use strong passwords, enabling file encryption, PIN enforcement, activity monitoring, device tracking, and the use of remote locking in the

event of the device being stolen or lost. The organisation should define what is considered acceptable use of the device for personal communication and other activities (such as the use of social networks) during company time.

The devices in use should be monitored, and if any violations are detected, they should be reported immediately. Role-based access control should be implemented. It is also highly recommended thata virtual private network (VPN) be employed which would keep secure the communications between devices and servers within the organisations network.

In the event that a device is lost or stolen, then the policy should dictate if the device should automatically be locked, and should it also be automatically wiped.It should have also previously been decided if it should be selectively wiped to remove corporate data only or all data to include personal data too (Absalom 2012).

For employees, should they be willing to use their own device in the workplace, then the policies in place should be made abundantly clear to them as to what this exactly means. They must have given explicit confirmation that they agree to have their device monitored and also given their consent for any security solution to be installed on their device (Absalom 2012; Tokuyoshi 2013).

It should also be made clear from the policy who is responsible for the technical support of the device. It should be decided beforehand, and also communicated, who is accountable for ensuring the latest security patches are installed and who ensuring that the OS and applications are up-to-date (Ernst & Young 2013).

SQ3. What is the current state of BYOD adoption by SMEs?

SME's have also been quick to allow BYOD to be adopted in their everyday business, but the problems can arise when they don't have as much money to invest in security procedures as a larger organisation might.

They are failing to invest in security awareness and information security programs for a number of reasons, which include a limited budget, a limited amount of time being spent educating employees of the dangers and threats to the business, and also there is a lack of appreciation of the risk facing SMEs. It has been noted that many mangers feel there business is too small to attract the attention of cyber criminals (Goucher 2011).

Many smaller businesses can be considered to be reactive and view solutions more in the shorter-term compared to larger companies (Grant et al. 2014). Many SMEs were not using the most common cyber security protection of implementing anti-virus programs because they do not think an attack will happen to them. Security is generally an afterthought for most SME's until an actual cyber-attack happens.

When a SME is looking to adopt BYOD, using mobile device management (MDM) solutions comes highly recommended. However, the cost associated with this software can be quite expensive and as a result could be out of the price range of many SME's.

In the following section, some solutions are offered to SME's who may be considering adopting BYOD but can't afford to pay for MDM solution to manage the policy.

SQ4. ***What solutions can be provided to assist the aforementioned IT professionals in SMEs?***

The cost of having a MDM service in operation can be quite expensive and restrictive for SME's. One service called AirWatch by the vender VMWare (VMWare 2014) prices their bundled services contracts between €2,000 to €7,000 initial installation costs, as well as an additional fee per device, meaning their prices could be out of the reach of some SME's. If a SME cannot afford the cost of a MDM solution, the following are security recommendations they can use to implement BYOD at a minimal cost to the organisation.

The following is a list of security recommendations which can be considered the minimum level of security designed to deal with the potential security risks with having BYOD in operation within an organisation. This list was developed using recommendations from the National Institute of Standards and Technology (N.I.S.T) and the Federal Bureau of Investigation (F.B.I) (NIST 2013; FBI 2013).

- Ensure devices are not jail-broken or rooted as doing so dramatically increases the risk of malware. Rooting is a process that allows you to attain root access to the operating system code
- Ensure that devices will self-lock as a period of inactivity so only those with knowledge of the pass code are able to unlock the device.
- Ensure anti-virus software is installed on all Android devices as it is the main defence against malware.

- Ensure all updates of operating system and applications are carried out immediately as these can help fix known vulnerabilities.
- Ensure all data on the device is encrypted as this makes it more difficult to access if the device becomes compromised.
- Ensure a passphrase is used to protect all devices as it makes accessing the device by intruders much more difficult.
- Ensure remote wipe capabilities are installed, so it is possible to erase data on any lost or stolen devices.
- Ensure data on the device is backed up on a regular occurrence.
- Ensure that apps are only installed from official app stores (Google Play, Windows Store, iTunes etc). No apps should be installed from un-trusted 3rd party app store as it is hard to ensure the app is safe when downloading from these sites.
- Ensure any communications carried out over Wi-Fi is done through a secure VPN.
- Ensure that there is a BYOD security policy in place. This should be a comprehensive policy that manages the use of mobile devices within the organisation so that employees know what is and isn't allowed on the organisations network.
- Ensure that employees are aware of their responsibilities and aware of the risks associated with using mobile devices. Employee training and security workshops should be carried out on a regular basis.

More Solutions for SMEs

Despite the small size of the company, and the possibility of a small IT department, there are some other things a SME can do to try and protect itself from the threats of having BYOD. These include ensuring two factor authentication is enabled on all devices and applications where possible, controlling access to the network and prioritizing the security concerns to ensure they get dealt with first (Todd & Rahman 2013). One advantage SMEs have over larger corporations is that the more personnel an organisation employs, the more vulnerable their network is.

The first action any enterprise wishing to enable BYOD adoption should be the adoption of a company wide security policy that would help to mitigate the exploitation of company data from theft by cyber criminals or by careless employees. The security policy that is implemented should ideally follow the guidelines laid out in the ISO/IEC 27000 family of standards, paying par-

ticular reference to the ISO 27001 framework (Murphy & Murphy 2013).The ISO/IEC 27000-series is the information security standards which have been published jointly by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC) and the ISO 27001 framework is the specification for an information security management system (ISO 2014).

While some frameworks do exist within SMEs, the reason for their adoption is sometimes unclear and that could range from a lack of education to the frameworks being too complex for the employees (Prince & King 2012). If the set of security frameworks can be applied correctly it will become the backbone of a company's security policy.

Employees should also be made to sign a compulsory waiver acknowledging that they are fully aware of company policies covering security, privacy and data protection issues. It would also be possible to include these policies in their contract to ensure that the company is legally covered (Navetta 2012b).

Should these recommended measures be put into place within a SME, then it would be possible for the SME to reap the benefits of BYOD, which would help ensure employee satisfaction and increasing productivity.

5 CONCLUSIONS

The thesis presented a systematic review of literature on the phenomenonof Bring your Own Device (BYOD), trying to pay particular attention to SMEs.

The aim of the work was to identify known policies for BYOD, as well as issues and challenges which arose from having this policy implemented by an organisation. Additionally, research was also carried out which looked at the effects of BYOD on SMEs. The review was conducted by following the guidelines of Kitchenham, Okoli and Schabram for conducting systematic reviews, and using thematic synthesis to analysis the literature. The search for relevant articles and papers was limited to those published between the years of 2009 – 2014, and the result was 36 papers which were analysed.

This thesis has tried to answer all the research questions which were outlined in the beginning in chapter 1.

Despite the perceived success of adopting BYOD in the workplace,there are still many issues which are being worked towards. BYOD has been seen to bring many benefit to organisations who adopt it, but it can also bring many additional risk, that if an organization is not fully prepared for, then it can devastating effects.

In order to be able to counteract these threats, organisations must be prepared from the start, and implement policies that will help protect themselves. Larger organisations can be seen to have an advantage as they may have a dedicated IT security teams in place to help them implement these policies. However, it is very important that organisations ensure that not only are the policies implemented, but that they are also followed by the employees, as the biggest threat comes from employees not following procedure. For example, if an employee was responsible for updating the anti-virus according to the policies, but fails to do so, then they may be putting the organisation at risk. It is important that all parties know what their responsibilities are, and that these responsibilities are fulfilled. Training should be provided for the employees not only at the beginning of their employment, but continuously throughout. Clear lines of communication must also be open between employees and IT staff in regard to keeping devices updated, and informed of any policy changes.

This research has also shown that SMEs must also be careful when BYOD to be used in their organisation allow. Some SME believe that cyber attacks are not a concern for them, but rather for the larger organisations, and as such have deficient security policies. It is important that these organisations realise that they need to be fully protected from attacks.

Despite not having a dedicated IT security team in place to implement BYOD, it is still possible for SMEs to do so. Mobile Device Management (MDM) can be seen as an ideal way to help implement BYOD through the services offered. However, some of these services can be considered expensive and not applicable to all SMEs, so these businesses should take great care when allowing employee devices on their network. A series of guidelines have been presented in the previous chapter which can assist SMEs in allow these devices to be used in work situations.

This thesis has come to the conclusions that there has not been enough focus by primary study researchers in this area. Also, in regards to the adoption of BYOD by SMEs specifically, this has been overlooked by researchers almost completely and is very much an area in need of investigation. The more research that is conducted in this area the more recommendations that will appear tohelp in the adoption of mobile devices by employees in the work place.

Finally, BYOD is still a relatively new phenomenon which needs time to mature. It is hoped that this thesis will help researchers to gain a better understanding of this trend.

5.1 FUTURE WORK

By using the results of this systematic review, some areas for further research can be identified. These areas can improve the understanding of the phenomena of Bring your own Device in a small or medium sized environment. The main areas this systematic review suggests for more-studies have been summarized by following.

• Investigation and study of BYOD specifically in a SME.

• Conducting more research on BYOD by academic researchers

• Investigating more interpersonal issues involved in BYOD and also the legal issues involved with privacy.

6 BIBLIOGRAPHY

Absalom, R., 2012. International Data Privacy Legislation Review: A Guide for BYOD Policies. *MobileIron*, (May), pp.1–23.

Absalom, R., 2011. The BYOD Gap : Trends , Strategy , and the State of Mobile Device Management. *MobileIron*, pp.1–25.

Apple, 2014. About the security content of iOS 7.1. Available at: http://support.apple.com/kb/HT6162 [Accessed April 19, 2014].

Astani, M., Ready, K. & Tessema, M., 2013. BYOD issues and strategies in Organizations. *Issues in Information Systems*, 14(2), pp.195–201.

Bankosz, G. & Kerins, J., 2014. Mobile Technology-Enhanced Asset Maintenance in an SME. *Journal of Quality in Maintenance Engineering*, 20(2), pp.1–22.

Barnett-Page, E. & Thomas, J., 2009. Methods for the synthesis of qualitative research : a critical review. *BMC medical research methodology*, 9(1), pp.1–26.

Chung, S. et al., 2012. 2TAC: Distributed Access Control Architecture for "Bring Your Own Device" Security. *2012 ASE/IEEE International Conference on BioMedical Computing (BioMedCom)*, (SocialInformatics), pp.123–126.

Cisco, 2011. *Cisco Connected World Technology Report*, Available at: www.cisco.com/en/US/netsol/ ns1120/index.html [Accessed April 12, 2014].

Cisco, 2012. *Cisco Study: IT Saying Yes To BYOD - The Network: Cisco's Technology News Site*, Available at: http://newsroom.cisco.com/release/854754/Cisco-Study-IT-Saying-Yes-To-BYOD [Accessed April 12, 2014].

Collins, J. & Fauser, B., 2005. Balancing the strengths of systematic and narrative reviews. *Human reproduction update*, 11(2), pp.103–4.

Cooper, H., Hedges, L. & Valentine, J.C., 2009. *The Handbook of Research Synthesis and Meta-Analysis*, Russell Sage Foundation.

Copeland, R. & Crespi, N., 2012a. Analyzing consumerization-Should enterprise business context determine session policy? In *16th International Conference on Intelligence in Next Generation Networks*. pp. 187–193.

Copeland, R. & Crespi, N., 2012b. Controlling enterprise context-based session policy and mapping it to mobile broadband policy rules. In *16th International Conference on Intelligence in Next Generation Networks*. pp. 194–201.

Cruzes, D. et al., 2007. Extracting Information from Experimental Software Engineering Papers. In *International Conference of the Chilean Computer Science Society*. p. 10.

Cruzes, D. & Dybå, T., 2011. Recommended steps for thematic synthesis in software engineering. In *Proc. of ESEM'11, Banff-Alberta*. p. 11.

Devos, J., Landeghem, H. Van & Deschoolmeester, D., 2012. Rethinking IT governance for SMEs. *Industrial Management & Data Systems*, 112(2), pp.206–223.

Disterer, G. & Kleiner, C., 2013. BYOD Bring Your Own Device. *Procedia Technology*, 9, pp.43–53.

Ernst & Young, 2013. *Security and risk considerations for your mobile device program*,

European Commission, 2014. Fact and figures about the EU´s Small and Medium Enterprise (SME). Available at: http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/index_en.htm [Accessed April 12, 2014].

FBI, 2013. Criminal Justice Information Services (CJIS) Security Policy. *Criminal Justice Information Services Division Criminal*.

Gammage, B. et al., 2010. *Gartner's Top Predictions for IT Organizations and Users, 2011 and Beyond: IT's Growing Transparency*,

Gheorghe, G. & Neuhaus, S., 2013. Preserving privacy and accountability for personal devices. In *CCS'13 Berlin*. Berlin, pp. 1359–1361.

Ghosh, A., Gajar, P. & Rai, S., 2013. Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, 4(4), pp.62–70.

Google, 2014a. Android KitKat. Available at: https://developer.android.com/about/versions/kitkat.html#44-security [Accessed April 19, 2014].

Google, 2014b. Fragmentation | Android Developers. Available at: http://developer.android.com/about/dashboards/index.html?utm_source=ausdroid.net [Accessed April 19, 2014].

Goucher, W., 2011. Do SMEs have the right attitude to security? *Computer Fraud & Security*, 2011(7), pp.18–20.

Grant, K. et al., 2014. "Risky business": Perceptions of e-business risk by UK small and medium sized enterprises (SMEs). *International Journal of Information Management*, 34(2), pp.99–122.

Harris, M. a. & Patten, K.P., 2014. Mobile device security considerations for small - and medium-sized enterprise business mobility. *Information Management & Computer Security*, 22(1), pp.97–114.

Hensema, M., 2013. Acceptance of BYOD among Employees at Small to Medium-sized Organizations. In *19th Twente Student Conference on IT*. pp. 1 – 8.

ISO, 2014. ISO 27000 - An Introduction to ISO 27001. Available at: http://www.27000.org/iso-27001.htm [Accessed June 8, 2014].

James, P. & Griffiths, D., 2012. The Mobile Execution Environment: A Secure and Non-Intrusive Approach to Implement a Bring You Own Device Policy for Laptops. In *Proceedings of the 10th Australian Information Security Management Conference,* . Perth, Western Australia: SRI Security Research Institute, Edith Cowan University, pp. 82– 91.

Kaplan, B. & Duchon, D., 1988. Combining qualitative and quantitative methods in information systems research: a case study. *MIS quarterly*, (December), pp.571–587.

Kaur, J. & Mustafa, N., 2013. Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 2013, pp.286–290.

Keyes, J., 2013. *Bring Your Own Devices (BYOD) Survival Guide*, Auerbach Publications.

Kitchenham, B., 2004. Procedures for Performing Systematic Reviews. *Keele UK Keele University (2004)*, 33(TR/SE-0401), pp.1 – 28.

Lennon, R., 2012. Changing User Attitudes to Security in Bring Your Own Device (BYOD) & the Cloud. In *Tier 2 Federation Grid, Cloud & High Performance Computing Science (RO-LCG), 2012 5th Romania*. IEEE CONFERENCE PUBLICATIONS, pp. 49 – 52.

Liu, L., Moulic, R. & Shea, D., 2010. Cloud Service Portal for Mobile Device Management. *2010 IEEE 7th International Conference on E-Business Engineering*, pp.474–478.

Mahesh, S. & Hooter, A., 2013. Managing and Securing Business Networks in the Smartphone Era. In *Fifth Annual General Business Conference, Sam Houston State University, Huntsville, Texas*. Texas: Management Faculty Publications.

Merriam, S.B., 2009. *Qualitative Research: A Guide to Design and Implementation*, John Wiley & Sons.

Mont, J., 2012. The Risks and Benefits of Employee-Owned Devices. *Compliance Week*, 103(9), pp.48–49.

Morrow, B., 2012. BYOD security challenges: control and protect your most sensitive data. *Network Security*, 2012(12), pp.5–8.

Moyer, J.E., 2013. Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage. *Journal of Hospital Librarianship*, 13(3), pp.197–208.

Murphy, D. & Murphy, R., 2013. Teaching Cybersecurity: Protecting the Business Environment. In *Proceedings of the 2013 on InfoSecCD'13*. Kennesaw, GA. USA, pp. 88 – 93.

Nasstar, 2012. Staff are happier if they can bring their own devices to work. Available at: http://www.nasstar.com/news/byod-survey [Accessed April 12, 2014].

Navetta, D., 2012a. The Legal Implications of BYOD (Part II) - Preparing Personal Device Use Policies. *Information Law Group*. Available at: http://www.infolawgroup.com/2012/06/articles/byod/the-legal-implications-of-byod-part-ii-preparing-personal-device-use-policies/ [Accessed April 26, 2014].

Navetta, D., 2012b. The Security, Privacy and Legal Implications of BYOD (Bring Your Own Device). *Information Law Group*. Available at: http://www.infolawgroup.com/2012/03/articles/byod/the-security-privacy-and-legal-implications-of-byod-bring-your-own-device/ [Accessed April 12, 2014].

NIST, 2013. 800-124 - Guidelines for Managing the Security of Mobile Devices in the Enterprise. *National Institute of Standards and Technology Special Publication*.

Okoli, C. & Schabram, K., 2010. Working Papers on Information Systems A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Sprouts: Working Papers on Information Systems*, 10(26), pp.1 –49.

PriceWaterhouse Cooper, 2012. UK Information Security Breaches Survey - Technical report. , (April).

Prince, D. & King, N., 2012. *Small Business : Cyber Security Survey 2012 Security Lancaster*, Lancaster: Lancaster University.

Ready, K.J., Astani, M. & Tessema, M., 2014. Human Resource Issues in BYOD Policy Development. *The Journal of Ameican Academy of Business*, 19(March), pp.40–47.

Rose, C., 2013. BYOD: An Examination Of Bring Your Own Device In Business. *Review of Business Information Systems*, 17(2), pp.65–71.

Sangani, N. & Vijayakumar, B., 2012. Cyber Security Scenarios and Control for Small and Medium Enterprises. *Informatica Economica*, 16(2), pp.58–72.

Scarfò, A., 2012. New Security Perspectives around BYOD. In *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications*. IEEE Conference Publications, pp. 446–451.

Seigneur, J. & Kölndorfer, P., 2013. A Survey of Trust and Risk Metrics for a BYOD Mobile Worker World. In *SOTICS 2013, The Third International Conference on Social Eco-Informatics*. pp. 82–91.

Silva, F.Q.B. Da et al., 2013. Using Meta-ethnography to Synthesize Research: A Worked Example of the Relations between Personality and Software Team Processes. *2013 ACM / IEEE International Symposium on Empirical Software Engineering and Measurement*, pp.153–162.

Singh, N., 2012. BYOD Genie Is Out Of the Bottle –"Devil Or Angel." *Journal Of Business Management & Social Sciences Research*, 1(3), pp.1–12.

Thomas, J. & Harden, A., 2008. Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC medical research methodology*, 8, p.45.

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

TNS Global Research, 2013. *Dell and Intel Study Concludes IT Consumerization Increases Productivity in the Workplace | Dell*, Available at: http://www.dell.com/learn/us/en/uscorp1/secure/2012-07-25-dell-evolving-workforce-report3 [Accessed April 12, 2014].

Todd, M. & Rahman, S., 2013. Complete Network Security Protection for SME's within Limited Resources. *International Journal of Network Secuirty & In Applications (IJNSA)*, 5(6), pp.1 – 13.

Tokuyoshi, B., 2013. The security implications of BYOD. *Network Security*, 2013(4), pp.12–13.

VMWare, 2014. AirWatch MDM pricing. Available at: http://www.air-watch.com/pricing [Accessed June 8, 2014].

Walker-Osborn, C., Mann, S. & Mann, V., 2013. to Byod or … not to Byod. *ITNOW*, 55, pp.38–39.

Walters, P., 2012. The Risks of Using Portable Devices. , pp.1–5.

Walters, R., 2012. The cloud challenge: realising the benefits without increasing risk. *Computer Fraud & Security*, 2012(8), pp.5–12.

Zielinski, D., 2012. Bring your own device. *HR Magazine-Alexandria*, 57(February), pp.71–74.