Bachelor degree Project

What Role does Top Management play in BYOD Policy Compliance?

Vilken roll spelar toppledningen i BYOD policyefterlevnad?

Bachelor Degree Project in Informatics
IT610G, G2E, 22.5 HP/Credits
Spring term 2021
Date of Examination: 2021-06-13

Student: Robin Klint
a18robkl@student.his.se

Supervisor: Dennis Modig
Examiner: Ali Padyab

Acknowledgements

To start with I would like to thank my supervisor Dennis Modig, and examinator Ali Padyab for their effort in helping me throughout the work of this thesis. They were both incredibly supportive and made this experience much more exciting and fun than I ever thought it would be. Having them by my side was greatly beneficial and gave me guidance in how to tackle this task and ensuring I had a proper structure to follow from start to finish. Thank you both. Furthermore, I would like to thank all the people that volunteered as interviewees.

Sammanfattning

Bring Your Own Device (BYOD) fortsätter öka i popularitet bland många organisationer. Problem, risker, och hot kopplade till denna enhetsstrategi har blivit noggrant studerat och diskuterat i många olika artiklar. Dock, rollen som toppchefer spelar i BYOD policyefterlevnad, är en aspekt som har blivit försummad och behöver ytterligare forskning. Toppchefers medverkan, stöd, och attityd mot informationssäkerhetsarbete påverkar anställdas intentioner att följa säkerhetspolicys. Därav, kasta ljus på effekten chefer och företagskultur kan ha, bedöms förmånligt för både organisationer såväl som deras ledare. En systematisk litteraturrecension utfördes med syftet att besvara vilken roll toppchefer spelar i BYOD policyefterlevnad. Specifika söktermer användes i fyra olika databaser för att hitta artiklar, som sedan utsattes för en process för att bedöma deras kvalitet baserat på förbestämda urvalskriterier. Denna process ledde till 14 artiklar som bedömdes vara bidragande till denna uppsats. Koncept som diskuterades och inträffade i flera av de valda artiklarna blev markerade och vidare analyserade. Fem koncept blev extraherade, och slutsatser drogs från dem. Fem intervjuer utfördes och resultaten både styrkte slutsatserna dragna från koncepten, och gav nya intressanta vinklar och aspekter.

Abstract

Bring Your Own Device (BYOD) continues to rise in popularity among many organisations. Problems, risks, and threats connected to this device strategy have been thoroughly studied and discussed in many different articles. However, top managers' role in BYOD policy compliance is an aspect that has been neglected and needs further research. Top managers' involvement, support, and attitude towards information security work affect employee's intentions to comply with security policies. Hence, shedding light on the effect managers and corporate culture can have is deemed beneficial for both organisations and their leaders. A systematic literature review was conducted to answer what role top managers play in BYOD policy compliance. Specific search terms were used in four different databases to find articles which were then put through a process to assess their quality based on pre-defined selection criteria. This process led to 14 articles that were deemed to be contributory to this thesis. Concepts that were discussed and occurred in several of the selected articles were highlighted and further analysed. Five concepts were extracted, and conclusions were drawn from them. Five interviews were conducted, and the results supported the conclusions drawn from the concepts and provided interesting new angles and aspects.

Table of Contents

1 Introduction 1

2 Background 2

2.1 Alternatives to BYOD 2

3 Problems & risks 3

3.1 Countermeasures 3

3.1.1 Technical 3

3.1.2 Organisational measures 4

3.2 Background to BYOD Policy 4

3.3 Latest BYOD research 4

4 Problem Formulation 5

4.1 Research Question 5

4.2 Research aim 5

4.3 Motivation 6

5 Methodology 6

5.1 Method 1 - Systematic Literature Review 6

5.1.1 Database Selection 7

5.1.2 Inclusion/Exclusion Criteria 7

5.1.3 Search strings 8

5.1.4 Article Selection Process 8

5.1.5 How to analyse results 10

5.1.6 Validity 12

5.1.6.1 Descriptive validity 12

5.1.6.2 Interpretative validity 12

5.1.6.3 Theoretical validity 13

5.2 Method 2 – Interviews 13

5.2.1 Data coding 14

6 Result of Literature Review 14

6.1 C1 – Communicating policies 14

6.2 C2 – Top Managers' Involvement, Support, Attitude 15

6.3 C3 – SMEs 15

6.4 C4 – Social Learning & Corporate Culture 16

6.5 C5 – Policies that guide behaviour 16

7 Results of Interviews 17

7.1 T1 – Communicating policies 17

7.2 T2 - Top Managers' Involvement, Support, Attitude 17
7.3 T3 - SMEs 18
7.4 T4 - Social Learning & Corporate Culture 18
7.5 T5 - Policies that guide behaviour 19
7.6 T6 - Passiveness (Emerged from Interviews) 19
8 Discussion 20
8.1 Execution of literature review process 20
8.2 Ethical and societal aspects 21
8.2.1 Ethical 21
8.2.2 Societal 21
8.3 Future work 21
9 Conclusions 21
10 Propositions 22

Appendix A - Interview Questions

1 Introduction

Bring Your Own Device or, (BYOD), is a term meaning that employees are allowed, or even encouraged to bring their personal laptops, smartphones, and other devices to work and use them to perform work tasks and connect to the company's network and other information resources. Some of the benefits of adopting this method of working are, according to Downer and Bhattacharya (2015), that it brings down hardware costs for the company since they do not have to buy new hardware for every employee, satisfies the employees, and increases their productivity. However, centralising the security on BYOD devices is hard since there could be many different types of devices with their own specifications, and the legal aspect of how much control or monitoring that is allowed to do on someone's personal device can be somewhat unclear. It can make it difficult to ensure all these devices are being used safely, and that they do not become attack vectors for possible attackers to exploit. This is something that there is a lot of already existing research about, with thousands of articles covering different attacks and security threats against BYOD-enabled environments, ways of mitigating attacks, and how employees should use their devices in a safe manner, which could argue that it would be unnecessary to engage in further research on that specific matter. Also, a lot of the research on the matter is focused on employees instead of people with managerial roles.

BYOD policies are often referred to as information security policies (ISPs) and Bulgurcu et al. define ISPs as *"a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations."* (2010, pp. 526-527). They also indicate that an ISP incorporates rules that cover security issues and instructions on what the employees are to do when they use their organisation's information and technology resources.

Palanisamy et al. (2020b) hint at a gap in the research of BYOD issues, being the impact that top managers have on BYOD policy compliance, which is the main subject this thesis aims to further analyse. Bulgurcu et al. (2010) point out that employees that do follow information security rules and regulations, set by the company, are *"the key to strengthening information security"*, which should make it even more compelling for top managers to try and understand policy compliance behaviour, and for more research to be done on this topic.

Thus, the research question in this paper is as follows: "What Role does Top Management play in BYOD Policy Compliance?"

This paper will be performed as a literature review to identify and give understanding as to what level of impact top managers have on BYOD policy compliance, combined with interviews with experts on this area for further insight to why there is a lack of support from top management for it.

2 Background

This chapter aims to cover existing research related to the subject of this thesis, which has contributed both to the forming of this work's research question and to help answer it. As earlier stated, a lot of research has been done about security issues, challenges and threats companies face when adopting the BYOD concept of working. A simple search for “byod security issues” on Google Scholar results in around 10 000 indexed articles. The following sub-chapters cover different aspects which have been studied in various research articles connected to BYOD issues, challenges, risks, etc. to give the reader of this work a greater understanding of the problem at hand.

The BYOD concept has been used in the workplace for several years now and is a continuously growing trend for companies within the information technology sector (Downer & Bhattacharya, 2015). Ratchford and Wang (2019) mean that with the rapid growth of IT consumerization, BYOD is something that organisations will just have to adapt to, i.e., it is not really in their hands to choose at this point. While adapting to BYOD might be necessary for many organisations, they should closely consider the different challenges and threats they could become susceptible to. Downer and Bhattacharya (2015) state that software-based attacks against mobile devices are increasing in rate. To mitigate attacks like these, organisations need to start with having security policies in place, set by managers or other authoritative roles. Even though this is something many studies have demonstrated, Kemper (2019) highlights alarming numbers from research done by “Switchfast” which states that 35% of employees and 51% of business leaders do not believe that their company is a target for cybercriminals. He also means that there is a relaxed attitude among company leaders, which is concerning.

Another aspect that companies must consider is employees' right to privacy when it comes to their working devices being owned by themselves. To what degree is the company allowed to monitor, control, and configure BYOD’s? Not paying attention to such questions, or generally breaking privacy rules and laws can generate legal issues for the company. These legal implications should not be overlooked when creating BYOD policies, but rather, they should be closely considered and included in the policymaking process (Alotaibi & Almagwashi, 2018).

With BYOD comes many advantages, both practical and theoretical. For the former, employees become more flexible and can choose to work from basically wherever they want because of the mobility of a smartphone/tablet. It also contributes positively to productivity and efficiency, reduces costs for the organisation which is connected to the lowered need for technical support (Alotaibi & Almagwashi, 2018). Seemingly it creates advantages for both employees and the organisation. However, with more personal devices used for work tasks comes the possibility for several different operating systems and settings which could make it more challenging to create security measures since a certain measure might not be as effective across all devices.

2.1 Alternatives to BYOD

Albeit being popular in many organisations, alternatives to BYOD such as CYOD (choose your own device) and COPE (corporate-owned, personally enabled) are also starting to become more popular. As the name suggests, CYOD gives the user a choice to choose what device he/she wishes to use as a work device, granted with some restrictions that the company will have set beforehand, but the company will pay for it. This also means that the organisation owns the device, but the user is allowed to use it for private usage, to some degree. According to Brodin

(2016), the benefits of CYOD are quite similar to BYOD in that it allows for flexibility, work outside of office hours and wherever you like, etc. He also points out that one of the biggest concerns with it is the lack of control over who can accidentally get a peak or, "shoulder surf", of the device when it is being used for work in public places.

In COPE policy the device is, just as in CYOD, owned fully by the company and the user can use it for personal matters as well. The main importance of this device strategy is the separation of corporate- and personal data (Rathnasekara et al., 2017). Something that differs COPE from BYOD and CYOD is that the user does not necessarily get to choose what device to use.

3 Problems & risks

Managers need to make employees get on board with the implementation of different security measures and policies on their BYODs to ensure a certain level of security, but employees are not always willing to allow this, which in turn increases the security and legal risks (Dhingra, 2016). Another aspect of this is that many employees seem to not even be aware of the existence of such policies in their organisations and even if they are aware of them, likely, they will not even bother to read through the policies. Timms states in his article that *"Recent surveys have shown only 39% of BYOD-enabled organisations have a policy in place, while 51% of BYOD employees said they've never read or seen a policy from their company."* (2017, p. 6). This all hints at another problem which is the way managers ensure that their employees are aware of and read through the policies that are set in place.

Not implementing the right safeguards for protecting sensitive data such as customer and financial data, is another crucial problem that can heighten the risks for lawsuits, large fines, and damaged company reputation (Tyler, 2016). Other problems and risks that can come with BYOD are technical attacks such as malware, phishing, hacking, and spoofing (Alotaibi & Almagwashi, 2018). However, these technical aspects have been widely covered in existing research articles and will therefore not be further discussed in this thesis.

3.1 Countermeasures

Policies, rules, and technological strategies can all be used to mitigate, or at least lower the amount and risk of threats, attacks, and tampering of company data and assets, but it is important in BYOD-enabled work environments to make use of both technological and organisational measures to achieve a good level of security and compliance (Kleiner & Disterer, 2015).

3.1.1 Technical

There are many technical tools that can be used to achieve a controlled and, to a degree, safe environment to work in with BYOD's. However, since this is not a focus in this thesis, only a few of them that are quite common will be covered.

Mobile Device Management (MDM) is a technological tool that provides control over applications, systems, and configurations in mobile devices and is important for companies to protect BYOD's. Most MDM programs make use of authorisation techniques to provision devices to be used as a work device and gives the option of creating group profiles with different settings fitting to a specific group. For example, a CTO might need access to certain files and services which some other employees do not, this is something group profiles can handle. The MDM

administrators will essentially have full control over the connected devices and so, have access to their data. Because of this, the organisation should make sure that these administrators can be fully trusted (Zahadat et al., 2015). When employees use their devices to work from home or other remote locations, a Virtual Private Network (VPN) connection can be used to be able to gain access to company resources in a controlled way and by doing so, allows for more work flexibility. Firewalls can monitor the network and detect and prevent malicious entities from entering the network (Downer & Bhattacharya, 2015).

3.1.2 Organisational measures

While there are technical measures to be taken towards achieving a safe BYOD environment, overseeing organisational measures could also be beneficial.

Vignesh and Asha (2015) propose a multilevel security policy that aims to improve security without decreasing productivity. It consists of three levels, namely "Organization level", "Application level", and "Device level". On the first level, BYOD policies should be made into a checklist, and shown to the employee, with the intent of clarifying certain things for the user such as that responsibility for backups of personal data lies on the user, removing apps upon request by the organisation is a must, device support, maintenance and costs and lastly cover consequences for any violations to the policy. This is something managers can do to ensure that they have completed the initial part of making their employees read through, and perhaps even sign a policy agreement. The next step in the authors' proposed model is to enforce access control based on the employees' responsibilities and job descriptions. This should be done to make sure that only authorised persons and devices get access to certain parts of the organisation's network and information assets.

3.2 Background to BYOD Policy

A security policy could potentially cover a vast majority of "dos" and "don'ts". In a BYOD-enabled environment, it is important to create a security policy that both considers and includes safeguards against threats and risks that come with BYOD. Some aspects to also consider are employee privacy, how to handle the mix of corporate data and the employee's data in a personal device, and legal implications and consequences (Alotaibi & Almagwashi, 2018). If a company has departments in different countries, or even globally, they also need to consider the differences in laws among the countries they are working in and adjust their BYOD policies accordingly (Downer & Bhattacharya, 2015). Furthermore, in addition to policies, making the employees' sign end-user agreements and liability agreements is a good way for companies to protect themselves in case of legal consequences from for example a security breach (Downer & Bhattacharya, 2015).

3.3 Latest BYOD research

As working from home is arguably the new norm, new concerning aspects arise connected to BYOD use. Scott et al. (2021) studied End of Life (EOL) in their article and to what degree organisations' BYOD policies cover this factor or not. The term refers to when a smartphone, laptop, or other similar device goes out of date, for example when security updates are no longer being released to the device, and how the disposal of this device is conducted. The worry being that corporate data remains on the discarded device. According to Scott et al. (2021), end-users often have a bad understanding of the concept of data-erasure, which contributes to a high

likeliness that sensitive data becomes remnant on old devices and that it could be used for malicious purposes. Their findings showed that only 32% of the organisations' BYOD policies addressed EoL, i.e., it is not covered by most organisations policies.

Koohang et al. (2020) studied the impact of different constructs that describe information security policy compliance, with one of them being role values. They refer role values to requirements within the guidelines of an ISP that are justifiable, acceptable, and related to the work performed by individuals. The researchers also studied several variables derived from the constructs, such as feeling guilty for not complying with ISP, morally wrong to violate the organisation's ISP, etc. They sent out a survey to faculty and staff at a mid-sized university in the USA and their results showed that role values had a significant impact on individuals' intention to comply with ISPs.

4 Problem Formulation

This chapter aims to shed light on the problem this research will study and showcase why the topic in this thesis is of importance and in need of studying. Further argumentation for the research question, research aim, and motivation is conducted in the following subchapters.

4.1 Research Question

Palanisamy et al. (2020b) states in their research that there is a gap in existing BYOD research, being the role that top managers in organisations play in getting their employees to comply with policies regarding how to use BYODs in a way that does not put them, or the company at risk for security issues. They also found out that high-ranking managers seemed to have a clearer understanding of the policies than the lower-ranking employees, which could be interpreted as a lack of communication skills between hierarchies in organisations. Those findings were discovered during a focus group discussion which also showed that enforcing policies that are so strong that it leaves the employee with little to no control over their devices, contributes to deliberate non-compliance. Being able to juggle a company's strictness in information security policies, employee satisfaction, and policy compliance is therefore important for managers.

Based on the problems discussed above, the research question is formulated as follows:

What Role does Top Management play in BYOD Policy Compliance?

4.2 Research aim

This paper will be performed first as a literature review to help answer the main part of the research question, which is the following: What exists and what is missing in top management support in BYOD policy compliance? Secondly, interviews will be performed to answer a second part, being 'why' there is a lack of support for BYOD policy compliance from top management positions. Together, these two angles will help contribute conclusions for what role top management play in BYOD policy compliance. For the literature review part, several scientific databases will be explored for the article selection process to try and cover as much research as possible, within a given time frame, and to ensure a certain level of validity. Articles will be used to help give a foundational understanding of what BYOD means and entails, its underlying security problems, what has already been studied, etc.

4.3 Motivation

The research question is of importance to answer for several reasons, with one being because the impact of top managers in employees BYOD policy compliance is, as explained by Palanisamy et al. (2020b), a gap in existing research done on the topic of BYOD and other intricately connected sub-topics. A lot of focus has been on the employees and what part they play in it all when it comes to ensuring a level of data security while working with their personal devices. And whilst that is of course of interest, it should be remembered that it is higher up in the hierarchy, namely with the top managers, that the rules and policies are created and should from there trickle down all the levels of employees in the organisation.

Even though so much study has been done on BYOD-security issues and challenges, threats, and ways of attacking a BYOD-enabled company will most likely only keep developing along with digitalisation paving its way forward in working environments. Continuing to shed light on different problem areas and gaps, such as the role of top managers in ensuring policy compliance, should therefore be of interest for both researchers, organisations, and their top managers (e.g., rule/policymakers). The following statement from Ameen et al. strengthens this argument; *"Top management play a critical role in managing information security and creating an organizational culture that encourages employees to keep their smartphones secure. Top managers influence employees' beliefs, which include their attitudinal, normative, and control beliefs"* (2021, p. 7). The authors also state that top managers' actions and behaviours can act as a determinant for the employee's security compliance behaviour.

Another interesting aspect to keep in mind is the effect of GDPR. GDPR is something top managers must take into serious account as it protects the individual employee and his/her personal data, in for example a BYOD, more than it does the company that wishes to implement data protective measures in said device. Barlette et al. (2021) mean that this is something that creates huge legislative, technical, and administrative challenges for managers and stresses the fact that it is the employer and not the employee that accepts full responsibility in case of breach of the GDPR regulations.

5 Methodology

This chapter covers and explains both methodologies used in this thesis and is divided into subchapters starting with the systematic literature review, all the steps taken within it, and showcasing its meta-results, followed by the second method i.e., semi-structured interviews.

5.1 Method 1 - Systematic Literature Review

Firstly, the research question was formulated in a way that it would be connected to the aim of the project. By doing so, it also helped to give a clearer direction in the process of searching and finding literature that is suitable for the topic. Kitchenham describes a systematic literature review as *"[a] means of identifying, evaluating and interpreting all available research relevant to a particular research question, or topic area, or phenomenon of interest"* (2004, p. 1). She also states reasons for performing this kind of review, with some of them being to identify gaps in existing research, summarise existing evidence, benefits, and limitations of a specific technology, and give some background that can contribute to new research activities. Since the topic of top managers' support in BYOD policy compliance is, as earlier stated, a gap in existing

research in BYOD policy compliance, and because of the arguments from Kitchenham (2004), the systematic literature review method was partially chosen for this thesis. Although Kitchenham (2004) includes a proposed method to conduct such a review, Jesson, Matheson, and Lacey (2011) provide a less complex and more straightforward approach that consists of the following six-step process:

1. Define the research question.
2. Design the plan.
3. Search for literature.
4. Apply exclusion and inclusion criteria.
5. Apply quality assessment.
6. Synthesis

Because of the less complex and more straightforward approach, this process was chosen.

The next steps include deciding over the databases to use, defining inclusion/exclusion criteria (Table 2.), and decide on keywords and search strings to be used when searching for articles in the databases (Table 3).

5.1.1 Database Selection

When scouring different databases for articles, it quite quickly becomes clear that many websites will charge the readers for several articles which would make it hard to conduct this thesis. Because of this, database websites have been entered from a list of databases to which the University of Skövde grants its students full access to most of their articles. The scientific databases used for this research have also been chosen with consideration to them being reliable in a way that they ensure all articles found on their websites are peer-reviewed. This is done to ensure a certain level of quality for this thesis. The resulting databases can be seen in Table 1.

Table 1. - Databases

Database	Website
IEEE - Institute of Electrical and Electronics Engineers	https://ieeexplore.ieee.org/Xplore/home.jsp
ScienceDirect	https://www.sciencedirect.com/
Tandfonline	https://www.tandfonline.com/
WebofScience	https://apps.webofknowledge.com

5.1.2 Inclusion/Exclusion Criteria

Wohlin et al. (2012) state that the inclusion and exclusion criteria are essential for the study selection process. They also point out that to avoid bias, this criterion should be created beforehand. This was done and the results can be seen in Table 2, but also further explained in this subchapter.

Articles were only included if they were peer-reviewed, which the selected databases all ensure, so that there is an assurance of their quality. They also had to be from 2015 and forward, this was decided for two reasons, one – to avoid the risk of articles that have become obsolete or irrelevant in time and, two – to create a feasible scope size.

All included articles should be written in English, and they should also have relevance to the

topic. Articles that do not meet these criteria are then excluded and the exclusion criteria consist of news articles, editorials, and other works that might be opinion-based, articles that require payment, and articles that have a bad language quality.

Some articles have been used, and referred to, in this project which are not exported from the same databases the other papers have been retrieved from. These articles are not part of the process that aims to answer the research questions but are instead only used for things like background information, description of methods, choosing of keywords/search strings, etc.

Table 2. – Inclusion/Exclusion Criteria

Inclusion	Exclusion
● Peer-reviewed articles from scientific databases ● Articles from 2015 and newer ● Written in English ● Have relevance to BYOD Policy Compliance	● Articles written in any other language than English ● News articles, editorials, or any other opinion-based works ● Require payment

5.1.3 Search strings

Keywords were created and embedded in search strings which were used when searching for articles in databases. Boolean Operators can be used to enhance the search results and some examples of such operators are AND/OR/NOT. The first one (AND), was used in this thesis and contributed to search strings such as “Byod AND compliance” and “Byod AND management”. This generates articles that include both words which make the search and its results more specific (Jesson et al., 2011). The resulting keywords and search strings can be seen in table 3.

Table 3. - Keywords & Search Strings

Keywords	Search Strings
● Byod ● Challenges ● Compliance ● Management ● Policy	● Byod policy compliance ● Byod AND challenges ● Byod AND compliance ● Byod AND management ● Byod AND policy management ● Byod AND policy

5.1.4 Article Selection Process

An iterative process was used for each search of articles in the databases in the form of rounds, with each round aiming to filter out irrelevant articles. Before starting this process, all the exported articles were entered in a bibliography software called “Mendeley” and checked for duplicates. This resulted in a total of 1092 articles with 238 duplicates, i.e., 854 articles after the removal of duplicates.

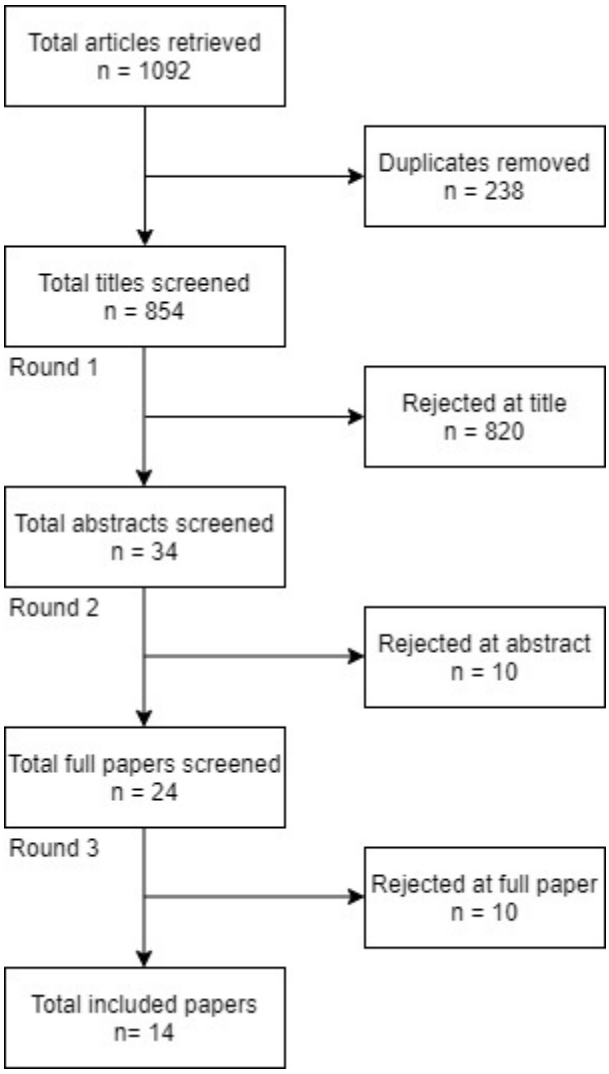

Figure 1. Flow diagram - Article selection process

In round one, titles of the exported articles were checked to decide if a good enough connection to the topic was existing. This amounted to the removal of 820 articles, and 34 kept.

In round two, abstracts were read through, and the articles passed the round if their abstracts made the paper seem relevant to the subject and contained a good language quality. In this step, 10 articles were removed, hence, 24 remained.

Round three meant reading through the articles to see if they were actually of importance for the research question. Granted, some of the articles were of partial importance meaning that not all information within them was directly connected to the subject. If they at least contributed to some angle of this research, they were kept. At first, most of the articles seemed to be of importance, but after reading through them a couple more times, it showed that some misinterpretation of their aim, results, or conclusions had taken place, resulting in going back to perform this step yet another time. This step ultimately resulted in the removal of 10 articles.

This three-step process resulted in 14 articles being considered valuable to the topic of this thesis and therefore being the ones used to help answer the research question. Tables 5 and 6 show the results of this process.

Table 4. - Exported Articles

Database	IEEE	ScienceDirect	TandfOnline	WebofScience
Exported Papers	122	490	390	90
Total with Duplicates	1092			
Total w/o Duplicates	854			

Table 5. - Rounds

Round	IEEE	ScienceDirect	TandfOnline	WebofScience	Remaining	Removed
1 (Title)	9	15	3	7	34	820
2 (Abstract)	7	13	1	3	24	10
3 (Full Article)	2	9	1	2	14	10

5.1.5 How to analyse results

When analysing the articles, it becomes clear that there are several similar concepts discussed. Watson and Webster (2020) imply that a literature review is "concept-centric", and therefore the concepts help create the framework, or process, of the review. Hence, their suggested method of mapping out discovered concepts in a concept matrix has been chosen for this thesis. To describe the method further, passages describing discovered concepts are highlighted and then further analysed and categorised. The categories that they create are then given a fitting title, which will be used in the concept matrix (see table 7), where each article is mapped to the concepts, they discuss. This is done to achieve a result of the most common concepts that are connected to the topic at hand, which we can then also use as contributors when drawing conclusions.

Table 6 - Concept Matrix

Articles	**Concepts**				
	Communicating policies from management to employees is necessary/can also positively affect policy compliance. (C1)	Top Managers' involvement/ support/attitude has a positive effect on employee's policy compliance. (C2)	SMEs are particularly vulnerable in BYOD environments, lack of top support/awareness of risks & threats. (C3)	Social learning/Environmental & corporate culture impact (C4)	Managers should create policies that guide employee's behaviour. (C5)
Nr. of Occurrences	**3**	**9**	**3**	**7**	**4**
(Alotaibi & Almagwashi, 2018)		**X**			
(Ameen et al., 2021)	**X**	**X**		**X**	
(Baillette et al., 2018)		**X**	**X**	**X**	
(Barlette et al., 2021)		**X**		**X**	
(Downer & Bhattacharya, 2015)					**X**
(Gokce & Dogerlioglu, 2019)			**X**	**X**	
(Hovav & Putri, 2016)		**X**			**X**
(Kemper, 2019)	**X**	**X**			
(Palanisamy, Norman, & Kiah, 2020a)		**X**		**X**	
(Palanisamy, Norman, & Mat Kiah, 2020b)		**X**		**X**	**X**

(Rostami et al., 2020)					**X**
(Timms, 2017)	**X**		**X**		
(Wang et al., 2017)				**X**	
(Zahadat et al., 2015)		**X**			

5.1.6 Validity

When it comes to the validity of research, it refers to the level of trustworthiness of the results and how the researcher came to those results. Wohlin et al. (2012) state that the reliability of the results and their level of truth and bias are symbolised by the validity of the research, thus, making sure to achieve a high level of validity is of importance. While Wohlin et al. (2012) give a clear definition of the importance of validity, their suggested methods to ensure validity are fitted towards quantitative research. To ensure validity throughout all steps in this thesis, being of a qualitative nature, recommendations have been followed from Hayashi et al. (2019) to adopt a processual approach. Furthermore, they explain that several different types of validity are to be considered with the most important being the following three types:

- Descriptive validity
- Interpretative validity
- Theoretical validity

5.1.6.1 Descriptive validity

Descriptive validity refers to the idea of not compromising information. Information and facts should not be altered or distorted by the researcher. In this thesis, an example of a threat like this could be that information extracted from the literature review process has been falsely cited or changed to better fit a narrative or desired result, or that what was said during the interviews has been falsely transcribed.

An example of mitigation for this threat is that proper referencing has been done when including cited text passages from articles. All interviews were recorded and have been thoroughly checked to avoid false translation and transcription.

5.1.6.2 Interpretative validity

The following quote from Hayashi et al. explains interpretative validity: *This refers to the researcher's sensitivity and mental processes in order to capture and interpret /construct the meaning of the objects, events and behaviors of the people engaged and involved in the studied phenomenon. Such validity encompasses the conscious processes, hidden intentions, beliefs, concepts, and values of the participants.* (2019, p. 100).

To mitigate this threat, the interviews were conducted with a semi-structured approach. This method includes having pre-defined interview questions that are open-ended which also allows for a freer conversation and does not put the interviewee in a corner where they feel pressured to answer with "yes/no", but instead lets them expand their answer and speak freely. Having pre-defined and easily understood interview questions. When an unclear or ambiguous answer was

given by the interviewee, control questions were asked by the interviewer to ensure a correct interpretation or understanding, of for example a concept, had been done.

5.1.6.3 Theoretical validity

Refers to how claims of concepts and categories have been created with the support of data. For example, if the claim is made that communicating policies to employees positively affect their compliance, the question is if that claim is backed up by the interview data? To mitigate threats of this nature, the results in this thesis have emerged from the articles used in the literature review and are further supported by interviews.

5.2 Method 2 – Interviews

The questions in Appendix - A were created with an intent to avoid one-word answers ("yes/no"), since such questions would not generate qualitative results and are perhaps more appropriate for questionnaires. A "semi-structured" approach was chosen for the interviews, in other words, the questions are "open-ended" and allow for a freer conversation between the interviewer and interviewee, which makes it possible to ask follow-up questions based on the given answers (Young et al., 2018). This method was chosen since part of the reason for the interviews was to gain more in-depth knowledge in addition to what the literature review could contribute. To ensure validity for the interviews, the same steps have essentially been followed as in the literature review process. Also, the formulated interview questions have been sent to the supervisor for this thesis, for a quality check, before conducting the interviews.

To achieve further insight as to what role top management plays in support for BYOD policy compliance, interviews were conducted with a selection of people who have researched on this area, worked in organisations that use BYOD, or consulted companies that wish to use BYOD in the workplace. Supervisor Dennis Modig and examinator Ali Padyab helped in the recruiting of interviewees process by suggesting people, administrations, or companies to contact. The interviews were between 20-30 minutes long, conducted in Swedish, and took place via the program Zoom, except for the first interview which was conducted via Microsoft Teams. Transcripts from these parts of the interviews will be included, translated to English, and further analysed in the next chapter. Identities of the interviewees will not be disclosed for privacy reasons, the same goes for the names of the companies they work for. The only thing disclosed will be their area of expertise, work background, and/or job title. When referring to the interviewees in the results chapter, *Expert X* will be used to further protect identities and avoid convoluted sentences, with *X* referring to chronological number ordering within which the interview took place. A total of five interviews were conducted and the questions asked can be seen in Appendix - A (with reservation for rephrasing or omitting questions if follow-up questions were deemed more appropriate). Table 7 contains some background information about each interviewed expert.

Table 7 - Interviewee/Expert Background

Interviewee/Expert	Background Information
1	Works as a "solution architect" at a company that specialises in IT infrastructure, delivering services and products to help customers with handling, operation, and development of their IT environments.
2	Has a twenty-year-long background in IT and information security and has worked as a consultant in that sector for almost ten years. Is

	currently working as an information security expert in several different organisations and is also CIO (Chief Information Officer) at a consulting company working with business and organisational change.
3	Works at a university as an information security coordinator, security officer, and has previously worked as an IT security manager within the armed forces.
4	Runs a company that consults organisations and companies to improve their IT security level.
5	Works as an information security coordinator in a municipality in Sweden.

5.2.1 Data coding

At the start of each interview, the researcher (being the author of this thesis) asked the interviewee to state their job title and give some background to what they have previously worked with or studied. This was done to ensure that an appropriate level of expertise on the subject was existing, and thus to ensure validity to the results. Concepts or arguments that the interviewees brought up were highlighted, analysed, and discussed in the form of themes in the following chapter.

6 Result of Literature Review

This chapter discusses the parts from the extracted articles that contributed to the resulting concepts seen in Table 7. In the concept matrix we can see that concept 1 "C1" appeared in three articles, "C2" in nine articles, "C3" in three articles, "C4" in seven articles, and "C5" in four articles. Hence, making C2 the most common concept. The following sub-chapters will further showcase the highlighted passages from the articles that contributed to the concepts, and conclusions will be drawn from them.

6.1 C1 – Communicating policies

C1 refers to the concept that communicating policies in a BYOD-enabled environment is necessary and can positively affect employee compliance.

According to Ameen et al. (2021), just having a policy is not enough, rather it needs to be effectively communicated throughout all departments and employees. Further, effective communication about cybersecurity will also have a positive effect on employees' intentional participation (Kemper, 2019).

An alarming problem is that many BYOD-enabled organisations do not have a policy in place, and even if they do, most employees are not aware of them (Timms, 2017). This further strengthens the argument that simply having a policy is not enough, but that it is vital to communicate them.

6.2 C2 – Top Managers' Involvement, Support, Attitude

C2 refers to the concept that top managers' involvement, support, and attitude have a positive effect on employee policy compliance.

Ameen et al. (2021) state that both employees' behavioural intention and their actual security compliance are affected by top management participation. This is interesting because if this participation only affected employees' intentions, but not their actual compliance, it would not necessarily be effective in practice. Another interesting aspect discussed by Baillette et al. (2018), is that the psychological state of top managers correlates with the involvement factor since the results of their participation efforts are affected by their sincerity.

Top management support can also be beneficial for managers that lack technical skills by providing more funding for the implementation of security measures, education, and campaigns for raising awareness. This kind of support can also contribute to the adherence of employees (Barlette et al., 2021).

Hovav and Putri (2016) discuss the importance of having an IT support team, and what impact it can have on employee's confidence in being able to perform actions stated in a BYOD security policy. They state that the availability of such a support team would contribute to a positive effect in increasing employees' perceived response efficacy and compliance behaviour.

Kemper (2019) implies that executives and managers can create a "trickle-down" compliance effect which can spread out to the whole organisation through embracement and allocation of resources to the policies. He also states that there is a correlation between the amount of provided leadership and the motivation of employees to work against cyber-crime.

Organisational culture can impact employees' attitude towards security policy compliance, which is something that Palanisamy et al. (2020a) mean that top management should consider since their participation is a factor that can help create a security culture that contributes to affect employees attitude towards policy compliance in a positive way. This connects both to C2 and C4 since it discusses the effect of management participation, or involvement, as well as the effect of environmental and corporate culture impact.

For an organisation to succeed in creating an alignment of their missions and security policy, Palanisamy et al. (2020b) implies that it is necessary to have committed top management that also defines the missions, goals, and strategy at an organisational level.

Zahadat et al. (2015) argue that organisations must continuously manage BYOD for as long as they use it to ensure identification and understanding of risks. They also state that the commitment on an executive level will "make or break" BYOD, i.e., top management support and involvement is important to maintain a safe BYOD environment.

6.3 C3 – SMEs

C3 refers to a suggestion that Small to Medium companies (SMEs) are particularly vulnerable when using BYOD, and that there is a lack of support and awareness of its risks and threats.

According to Baillette et al. (2018), SME CEOs do not have the technical and financial resources needed and often also lack the qualification to handle technologies in the right way, nor security issues. This is further corroborated by Gokce and Dogerlioglu (2019) who state that the lack of knowledge, within small-scale organisations, in implementing appropriate security strategies

contributes to security challenges when adopting BYOD.

Timms (2017) means that a negative consequence of this is that cyber hackers are aware of SMEs lack of resources to properly defend themselves, thus making SMEs a favourable target for cyber-attacks since they will most likely face less resistance.

6.4 C4 – Social Learning & Corporate Culture

C4 refers to the concept of social learning which, in this context, means the ability to learn how to conduct actions that comply with BYOD policies from social surroundings such as other employees. It also refers to the impact of two factors, namely the organisation's environment, and corporate culture.

Baillette et al. (2018) describe BYOD as a "reversed IT adoption logic", meaning that it is a work strategy that managers have not originally initiated. In their article, they talk about the importance of creating an organisational environment that preserves sensitive information and where employees are motivated to ensure the use of security measures that protects both their own information as well as the organisations in their BYODs. They also argue that this is a change that must be driven by the CEO.

Barlette et al. (2021) shares the same definition of BYOD as being a reversed IT adoption logic and discusses the ways corporate culture can impact employee's compliance behaviour, stating that managers possess the position from which they can intervene in corporate culture which can create positive changes in employees' attitude for compliant and secure behaviour. Managers can put these changes in motion by educating employees on how to improve security behaviours. Furthermore, the authors suggest creating a "BYOD-specific charter" that explains the risks and responsibilities that come with using your personal device, along with what to do if the device is lost or breaks. This charter should then also be signed by the employee.

To create the most effective security strategy for BYOD use, Gokce and Dogerlioglu (2019) suggest that an organisational environment within which top management, security staff, and end-users have a close collaboration is essential. Palanisamy et al. (2020a) touches on this subject as well, stating that employees rely on the organisational environment and in particular their managers and colleagues which have a big impact on their security behaviour.

According to Palanisamy et al. (2020b), when employees have received little or no training for mobile devices, employees will rely on their social surroundings for advice. They mean that this further shows the impact and effect of a social environment in the workplace since it can influence the employee's security compliance behaviour. They also state that employees learn from these social environments through observations, limitations, and social cues.

Wang et al. (2017) studied factors that drive employee participation in corporations that use BYOD and how it differs between a few countries. They found that in a BYOD program there is a positive association between social influence and participation intention, meaning that people that come from a strong collective culture, like China, are more likely to comply with opinions from important people such as their managers.

6.5 C5 – Policies that guide behaviour

Hovav and Putri (2016) examined employees' intention to comply with organisational BYOD policies and suggest the use of a security awareness program named SETA in BYOD-enabled

environments. The effect of SETA is that it *"positively influences users' attitude toward compliance with ISSPs and reduces perceptions of fairness restrictions"* (Hovav & Putri, 2016, p. 40). Granted, a SETA program is not a policy, but it is a program that is meant to promote employee's awareness when it comes to their rights and responsibilities, which in turn positively affects their compliance in a guiding manner. Palanisamy et al. (2020b) further highlights the importance for organisations that use BYOD to create security measures and privacy policies that guide employees behaviour which is something that Rostami et al. (2020) strengthen by arguing that the users of security policies, for example, employees, need to know what to do, how to act, and how to behave accordingly with the organisation's security requirements, i.e., information security policy users should get advice on how to conduct their tasks in relation to information security.

Downer and Bhattacharya (2015) mean that BYOD policies should also include guidelines for how to handle situations where employees do not comply, use their devices for illegal activities, or showcase difficulties in using their devices, which is seemingly guidelines for the managers or bosses to make use of since they would be responsible to handle such situations.

7 Results of Interviews

The results of the interviews are structured and partly based on the concepts found in the literature review process and are presented in sub-headings as themes. While most of the themes are connected to the concepts, as suggested by the heading such as "Theme 1 – C1", some new themes emerged from the interviews and are also analysed.

7.1 T1 – Communicating policies

The following is a quote from *Expert 1*: *"The CEO has a key role in being able to communicate the weight and mandate that 'now these are the rules'* (referring to security policies and regulations for BYOD). *It will be a bit of dictatorship, but it is a question of taking responsibility for the companies information."*

This indicates that company leaders are in the prime position from where they can spread the importance of their security policies and rules of how to work with BYOD, by communicating them. Also meaning that even if it might seem like a bit of dictatorship, the need for keeping company information safe might outweigh that.

Expert 2 suggested that security policies should be a living document that needs to be up to date and that it should be given out to employees and read by them yearly to also keep the employees up to date.

Expert 5 adds to this aspect, meaning that companies using BYOD need to have security policies that actually support BYOD, which is something far from all organisations have, and that they are agile so they can keep up to date with new BYOD devices.

7.2 T2 - Top Managers' Involvement, Support, Attitude

All experts meant that it is incredibly important to get the leaders' support in policy compliance work because the way they follow their own security policies will affect the way employees comply with them. Meaning that you can never expect employees to follow policies if they see

that their leaders do not. *Expert 2* supports this argument as well and adds that it is important that the support is being shown through all the levels of bosses and managers. Meaning that if one manager ignores the policies, chances are that behaviour will spread to other potential managers in different departments.

When asked how important Top Managements role is in creating a culture, within which work is being conducted in a safe manner, *Expert 5* answered that the Top Managements commitment is "completely decisive".

> *The Top Managements commitment to this is completely decisive, both what they say and signal but also how they themselves act, and this needs to come from the Top Management and needs to 'rain down' through the organisation, through the whole delegation order downwards, so that all subordinate managers have this self-evidently. So, it is completely decisive.*

7.3 T3 - SMEs

Expert 1 means that both small and large companies can be of interest for hackers to attack but that in SMEs, chances are higher that an attack would become successful since the IT maturity is often low, and that resources might not be enough to be able to have a dedicated IT department. Also adding that if these companies appoint someone responsible for IT security, it is quite often someone who lacks the necessary knowledge and skills, which could also be a contributory fact as to why SMEs become an interesting game for hackers.

While *Expert 4* also thinks that SMEs often do not have enough resources to allocate to an IT department, *Expert 4* suggests that large companies might be more interesting for some hackers.

> *Small to medium-sized companies often do not have the resources to allocate so much money to IT security, but the large companies that perhaps have allocated a budget for it, they might be a more interesting object for the ones who want to get access and could then get more attacks. But that probably depends mostly on what the company does.*

Since this was a new aspect that had not emerged from any of the articles processed in the literature review, a follow-up question was asked to see if *Expert 4* meant that it might be easier to perform a successful attack against SMEs but that more attacks occur against larger companies, to which the answer was *"yes"*.

7.4 T4 - Social Learning & Corporate Culture

What *Expert 2* said connected to C2, that if one manager ignores the policies it might generate a behaviour that will spread throughout the company, also relates to C4 in that there is a need for managers to show support and compliance with the organisations own policies, it could be seen as creating a corporate culture in which "we shall all follow the policies as a standard". Furthermore, *Expert 2* suggested that employees will do as their leaders do, not as they say. On this subject, *Expert 2* means that it is important to "sell" the importance of working securely to people within the company so that they understand it, which can contribute to them being able to think for themselves and make better, i.e., more secure decisions, meaning that this is a better way of reaching the goal of getting employees to comply with working in a safe way rather than relying on a lot of written policies that people might not read anyway. *Expert 4* added this and said that it is important to create the interest in working safely and compares the necessity of security

education, in a BYOD environment, as being similarly important as at a construction site, i.e., "wear a helmet!".

Expert 3 talked about the impact of *"signal values"*, referring to behaviour actions, performed by leaders in companies, that are seen by employees around them.

> *What managers, and especially top managers, do will set the agenda for a whole organisation. So, it is absolutely so that signal values, that are perhaps more informal and perhaps not written down in policy documents and such things even if they are of course good because they are what you might lean on, it is incredibly important that top management always acts with awareness since it sends such clear signals and they could spread in any direction.*

The term "signal values" used by *Expert 2* can be connected to what *Expert 2* said about employees doing as their leaders do and not as they say. Hence, for managers' it is important to consider their actions since they might have a bigger impact than one would think.

7.5 T5 - Policies that guide behaviour

Expert 4 suggested that a policy could be seen as a regulatory document that does not go into very deep detail on practicalities when it comes to how to conduct work tasks. Instead, it should be something that gives an overview of how the company and its leaders want and strives to conduct their work, not going into detail on things like how to identify a malicious weblink. Practicalities like that should then rather be taught through education. Combining that with policies that guide the user to understand how to work alongside the company's beliefs and goals is a strategy *Expert 4* recommends.

Expert 5 talked about policies and regulation documents being fundaments, but that complying with them is a question of cultural impact.

> *Regardless of Bring Your Own Device, regulatory documents and policies are fundaments themselves but to comply with them is a question of culture* (referring to corporate culture impact) *and that is very important, regardless of what aspect of security you talk about. So, if you are to get everyone to comply, then it needs to be an obvious natural part of how you think about your work in a security situation. So, to build culture is very important regardless of what aspect you talk about.*

7.6 T6 - Passiveness (Emerged from Interviews)

When asking *Expert 2* whether there is a lack of support from top management in getting their employees to follow BYOD policies, and if so, why? A new aspect emerged which can be seen in the following quote.

> *Laziness. They think it is more flexible to not follow it.*

Furthermore, *Expert 2* suggested that people higher up in the company hierarchy might feel they stand above some of the policies, that their work is more important, and that it would take too much time to follow the policies that taking some shortcuts would not generate such huge risks. Lastly, *Expert 2* stated that a problem with this is that everybody has a lot to do, meaning that it is not a feasible strategy.

Behaviour like this could spread through other departments and employees in the organisation,

which connects this theme of passiveness to concept 4 in that it could be seen as creating a social and corporate environment within which a passive attitude towards security policies emerges.

8 Discussion

This chapter will discuss how it went conducting the systematic literature review process and the interviews. Problems and changes in the initially decided strategy will also be discussed. Furthermore, ethical, and societal aspects will be covered followed by suggestions for future work connected to this thesis subject.

8.1 Execution of literature review process

The systematic literature review process conducted in this thesis consisted of several sub-steps that were done before the actual reviewing process began such as planning the review regarding formulating the research question, choosing databases, creating inclusion/exclusion criteria, defining search terms, etc. Deciding and defining these pre-steps proved to not be as time-consuming as initially thought. However, starting to actually perform the steps one by one was much more time-consuming. A reason for this was perhaps due to lack of experience in conducting a work of this magnitude and therefore became a bit overwhelming at first. But with the help and guidance of my supervisor and examinator, I quickly got more comfortable and found a good work rhythm and structure which showed itself to be quite efficient. Using the bibliography tool "Mendeley" was hugely beneficial as it is a user-friendly and neat tool that helps generate a structured library of all your articles and includes a Microsoft Word plugin that allows you to quickly insert references into your Word document. It can also help to find duplicates, highlight text passages with different colours, show PDFs so that one can integrate the article's files and directly read them in the same program.

Exposing the articles to the "rounds" was effective in assessing the quality of the exposed articles. However, it became less time-efficient than initially thought. Reading through the titles and abstracts went quite fast but reading through the articles fully took quite some time. Sometimes it was needed to go back and read through articles again to see if I had correctly interpreted their aims, findings, and conclusions which resulted in further removal of some. This could have been due to me gaining a better grasp and knowledge of the topic at hand while coming further along in the thesis.

The results from this method, i.e., the concepts, proved to acknowledge what some articles had already touched on. However, putting together the different aspects of each article's view on a certain concept is what ultimately led to the specific conclusions and propositions this thesis makes. That top management needs to consider the impact of their behaviour on employees' policy compliance is something many of the articles talked about, also that written policies are no silver bullet in information security work seemed to be something most researchers agreed upon. A new aspect that emerged from the interviews however was what *Expert 2* said about passiveness being a reason as to why there is a lack of support from top management in getting employees to comply with BYOD policies. This is alarming because of what was also discovered about how easily the behaviour from leaders spread throughout the company and could be something to conduct further research on.

Even though this thesis used a qualitative approach, it was interesting to get somewhat of a quantitative result in form of how frequently the different concepts were discussed in the exported

articles. C2 – Concept 2 was the most frequent and while the frequency on its own cannot be used to draw a solid conclusion of its importance, it is however interesting that each interviewee supported and/or further explained it to be one of the most important aspects for top management to consider.

8.2 Ethical and societal aspects

The following sub-chapters aim to cover the possible effects this thesis could have on ethical and social aspects.

8.2.1 Ethical

As BYOD continues to be a popular device strategy in many companies and as earlier stated, being something that most managers will just have to embrace, shedding light on different security problems connected to it is beneficial for organisations and their top managers. However, while showcasing that for example SMEs that use BYOD are more prone and vulnerable to cyber-attacks can contribute to managers in such companies to give extra thought to the matter, it might also inform malicious hackers that their attacks might be more likely to succeed if targeting a smaller company. Hopefully, this thesis can be beneficial to both top managers, CTOs, IT managers, and employees and in another aspect, contribute to other future studies done on a connected or similar topic.

8.2.2 Societal

This thesis is deemed necessary in that it discusses the reasons why top management should show commitment to ensuring BYOD policy compliance by having highlighted and analysed the impact their actions can have on employee's compliance behaviour. Also, including aspects such as why there is a lack of support from top management in BYOD policy compliance. By increasing and spreading the understanding of this subject, it can help organisations change their strategies when it comes to creating a safer environment both for the employees and the companies interests and assets.

8.3 Future work

Future work connected to the subject of this thesis could focus on how ensuring BYOD policy compliance differs in a time like now when more and more employees are working from home due to Covid-19, and what new aspects companies need to consider when updating their BYOD policies to be adapted to working from distance. To conduct further research on "passiveness" as a reason for there being a lack of support from top management in getting their employees to comply with security policies, could also be of interest.

9 Conclusions

In this thesis, a systematic literature review is conducted in combination with interviews to answer the following research question: What role does top management play in BYOD policy compliance.

In the first method, i.e., the systematic literature review, four scientific databases are searched for

articles. The articles are searched for with pre-defined search terms and selection criteria. The exported articles then go through an evaluation process that aims to ensure that a certain level of quality exists, and articles that do not meet the criteria are discarded. The articles that remain are then further analysed to discover concepts that contribute to conclusions. The second method, i.e., semi-structured interviews, are conducted with different experts on the subject to see if they support the concepts and arguments from the literature review, and to possibly contribute with new aspects or concepts that did not emerge from the first method.

Conducting these two methods have ultimately led to the following outcome:

- The most reoccurring concept that emerged from the literature review is "C2", which states that top management's involvement, support, and attitude have a positive effect on employee policy compliance. This concept is also supported by all six interviewees. And is therefore deemed as the most important concept for company leaders to consider.
- Top management in organisations using BYOD should closely consider focusing more on creating a corporate culture that encourages its employees to conduct work tasks in accordance with their security policies since this has an arguably stronger positive impact on policy compliance than simply letting employees read them.
- There is a general lack of support from top management when it comes to getting employees to comply with BYOD policies. This can stem from different aspects such as not possessing the knowledge about risk and threats that come with BYOD, lack of technical knowledge, passiveness, etc. SMEs are especially prone to security threats connected to BYOD because of a lack of financial resources to appoint a dedicated IT department and a lack of support and knowledge from top management to work with IT-security-related questions.

Based on the outcome presented above, the conclusion is drawn that top management plays a key role in BYOD policy compliance and hence, they find themselves in a position with the utmost power to induce change by possessing the ability to make decisions that can contribute towards a corporate culture within which all workers, regardless of title, work safely by complying with security policies and are encouraged to do so.

10 Propositions

Here, propositions will be made for top managers based on the empirical data and results from this thesis. The propositions are mostly based on the results from the literature review, i.e., the emerged concepts, as they are deemed to be the main contributions from this thesis. However, it should be remembered that they were all supported by the interviewees, which shows some additional weight of importance. This chapter aims to give some practical recommendations to companies that use BYOD, and their top managers.

- Effectively communicating policies in a BYOD-enabled environment to all departments and employees is of utmost importance. Simply having a policy is not enough and is, therefore, something top management should consider and work on.

- The involvement/support/attitude from top management is important in a BYOD-enabled environment and has a positive effect on employee policy compliance. Top managers should therefore consider their behaviour in these aspects.

- SMEs are particularly vulnerable to threats and risks of BYOD because of managers' lack of technical knowledge, skills, and limited resources. Hence, top managers in such organisations should consider allocating more resources to a proper IT department or IT manager with the necessary skills and knowledge.

- Social learning, organisational environment, and corporate culture can have a positive impact on employees' security and compliance behaviour and should therefore be taken into consideration by the CEO and Top Management.

- Managers within BYOD-enabled organisations should create policies that guide employees/end user's behaviour regarding information security.

References

Alotaibi, B., & Almagwashi, H. (2018). A Review of BYOD Security Challenges, Solutions and Policy Best Practices. *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, 1–6. https://doi.org/10.1109/CAIS.2018.8441967

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, *114*, 106531. https://doi.org/https://doi.org/10.1016/j.chb.2020.106531

Baillette, P., Barlette, Y., & Leclercq-Vandelannoitte, A. (2018). Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users. *International Journal of Information Management*, *43*, 76–84. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2018.07.007

Barlette, Y., Jaouen, A., & Baillette, P. (2021). Bring Your Own Device (BYOD) as reversed IT adoption: Insights into managers' coping strategies. *International Journal of Information Management*, *56*, 102212. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2020.102212

Brodin, M. (2016). BYOD vs. CYOD : What is the difference? In P. I. Miguel Baptista Nunes Philip Powell (Ed.), *9th IADIS International Conference Information Systems, 9-11 April 2016, Vilamoura, Portugal* (pp. 55–62). IADIS Press. http://his.diva-portal.org/smash/get/diva2:920380/FULLTEXT01.pdf

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. *MIS QUARTERLY*, *34*(3, SI), 523–548.

Dhingra, M. (2016). Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). *Procedia Computer Science*, *78*, 179–184. https://doi.org/https://doi.org/10.1016/j.procs.2016.02.030

Downer, K., & Bhattacharya, M. (2015). BYOD Security: A New Business Challenge. *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, 1128–1133. https://doi.org/10.1109/SmartCity.2015.221

Gokce, K. G., & Dogerlioglu, O. (2019). ``Bring your own device{''} policies: Perspectives of both employees and organizations. *KNOWLEDGE MANAGEMENT \& E-LEARNING-AN INTERNATIONAL JOURNAL*, *11*(2), 233–246. https://doi.org/10.34105/j.kmel.2019.11.012

Hayashi, P., Abib, G., & Hoppen, N. (2019). Validity in Qualitative Research: A Processual Approach. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2019.3443

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, *32*, 35–49. https://doi.org/10.1016/j.pmcj.2016.06.007

Jesson, J., Matheson, L., & Lacey, F. M. (2011). *Doing your literature review: Traditional and systematic techniques*. https://books.google.de/books?hl=en&lr&id=LUhdBAAAQBAJ&oi=fnd&pg=PP1&dq=Jesson,+J.,+Matheson,+L.,+%26+Lacey,+F.+M.+(2011).+Doing+your+literature+review:+Traditional+and+systematic+techniques.&ots=lD5piBEXVk&sig=6_M0-9U78ujrHFzvHEtJOI5TbXs#v=onepage&q&f=fa

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, *2019*(8), 11–14. https://doi.org/https://doi.org/10.1016/S1361-3723(19)30085-5

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele*

University, *33*(2004), 1–26.

Kleiner, C., & Disterer, G. (2015). Ensuring Mobile Device Security and Compliance at the Workplace. *Procedia Computer Science*, *64*, 274–281. https://doi.org/https://doi.org/10.1016/j.procs.2015.08.490

Koohang, A., Nord, J. H., Sandoval, Z. V, & Paliszkiewicz, J. (2020). Reliability, Validity, and Strength of a Unified Model for Information Security Policy Compliance. *Journal of Computer Information Systems*, 1–9. https://doi.org/10.1080/08874417.2020.1779151

Palanisamy, R., Norman, A. A., & Kiah, M. L. M. (2020). Compliance with bring your own device security policies in organizations: A systematic literature review. *Computers and Security*, *98*, 101998. https://doi.org/10.1016/j.cose.2020.101998

Palanisamy, R., Norman, A. A., & Mat Kiah, M. L. (2020). BYOD Policy Compliance: Risks and Strategies in Organizations. *Journal of Computer Information Systems*, 1–12. https://doi.org/10.1080/08874417.2019.1703225

Ratchford, M. M., & Wang, Y. (2019). BYOD-Insure: A Security Assessment Model for Enterprise BYOD. *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*, 1–10. https://doi.org/10.1109/MOBISECSERV.2019.8686551

Rathnasekara, C., Athukorala, T., Dikwellage, L., Wickramasuriya, U., Senarathne, A., & Elvitigala, S. (2017). Securing corporate data in mobile devices in a COPE environment. *2017 6th National Conference on Technology and Management (NCTM)*, 120–125. https://doi.org/10.1109/NCTM.2017.7872839

Rostami, E., Karlsson, F., & Gao, S. (2020). Requirements for computerized tools to design information security policies. *Computers & Security*, *99*, 102063. https://doi.org/https://doi.org/10.1016/j.cose.2020.102063

Scott, B., Mason, R., & Szewczyk, P. (2021). A Snapshot Analysis of Publicly Available BYOD Policies. *2021 Australasian Computer Science Week Multiconference*. https://doi.org/10.1145/3437378.3437394

Timms, K. (2017). BYOD must be met with a wider appreciation of the cyber-security threat. *Computer Fraud & Security*, *2017*(7), 5–8. https://doi.org/https://doi.org/10.1016/S1361-3723(17)30058-1

Tyler, J. (2016). Don't be your own worst enemy: protecting your organisation from inside threats. *Computer Fraud & Security*, *2016*(8), 19–20. https://doi.org/https://doi.org/10.1016/S1361-3723(16)30063-X

Vignesh, U., & Asha, S. (2015). Modifying Security Policies Towards BYOD. *Procedia Computer Science*, *50*, 511–516. https://doi.org/https://doi.org/10.1016/j.procs.2015.04.023

Wang, X., Weeger, A., & Gewald, H. (2017). Factors driving employee participation in corporate BYOD programs: A cross-national comparison from the perspective of future employees. *AUSTRALASIAN JOURNAL OF INFORMATION SYSTEMS*, *21*.

Watson, R. T., & Webster, J. (2020). Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0. *Journal of Decision Systems*, *29*(3), 129–147. https://doi.org/10.1080/12460125.2020.1798591

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Systematic Literature Reviews BT - Experimentation in Software Engineering* (C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, & A. Wesslén (eds.); pp. 45–54). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-29044-2_4

Young, J., Rose, D., Mumby, H., Benitez-Capistros, F., Derrick, C., Finch, T., Garcia, C., Home, C., Marwaha, E., Morgans, C., Parkinson, S., Shah, J., Wilson, K., & Mukherjee, N. (2018). A methodological guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution*, *9*, 10–19. https://doi.org/10.1111/2041-

210X.12828

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, *55*, 81–99. https://doi.org/https://doi.org/10.1016/j.cose.2015.06.011

Appendix A - Interview Questions

The interview questions referred to in chapter 7 are the ones below. As briefly explained in chapter 7, these are the pre-prepared base questions for the interviews. However, not all of them were necessarily asked in the exact way they are written here but were instead sometimes altered or omitted depending on if follow-up questions were deemed more appropriate based on the answers given by the interviewee.

1. What are, according to you, the biggest security concerns for organisations that use BYOD?
2. In what ways can a manager, or boss, ensure that the employees abide by the security policies for using their personal devices to conduct work tasks?
3. Should there be different policies based on what role and responsibilities one has, and if so, what are the pros and cons with that?
4. Is it possible for a manager, or boss, to ensure that policies are fully followed, or is it worth more to allocate time and money to educate staff about risks, threats, and consequences that are connected to BYOD?
5. What role does Top Management play in getting their employees to follow BYOD policies?
6. Is there a lack of support from Top Management in getting their employees to follow BYOD policies, and if so, why?
7. Many articles state that SMEs are particularly prone to cyber-attacks. Why do you think this is, and do managers in such companies lack the necessary knowledge and technological skills to handle IT security?