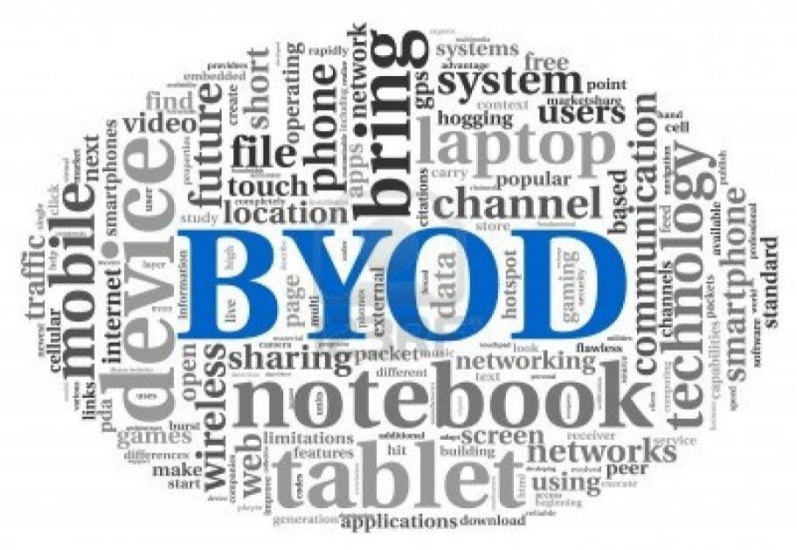
SECURITY RISKS ASSOCIATED WITH BYOD

Master Thesis Winter 2016



WRITTEN BY:
AHMAD KADER BAIS

SUPERVISORS:
PROF. KNUD ERIK SKOUBY
ASST. PROF. SAMANT KHAJURIA

BUSINESS DEVELOPMENT TRACK
ICTE AALBORG UNIVERSITY COPENHAGEN

Acknowledgements

The master thesis entitled ‘BYOD-Security’ is submitted to Business Development Track at the Department of ICTE, Aalborg University Copenhagen Denmark. The thesis investigates BYOD concepts, technologies, security issues and its sustainability issues. The period of the thesis was from 1st of Jun 2016 to 15th of November 2016.

The good support and guidance from the two supervisors Prof. Knud Erik Skouby and Asst. Prof. Samant Khajuria at the department of Electronic Systems in AAU, Copenhagen is highly acknowledged. Their comments and suggestions have greatly played a motivational role to work during the thesis and it has been reflected in the outcome of the research. The vendor, Cisco is highly thankful for providing me an opportunity for a valuable interview session; as well as both office of UNDP in (Denmark & Bosnia-Herzegovina) for giving me an opportunity to have an interview with their departments. The information from the interview helped me in the case study of BYOD and having an overview of BYOD illustration in a great way. A special gratitude to my friend Suman he is working at UNDP Copenhagen department he helped me to arrange an interview in UNDP department with Moe Kyaw.

Lastly, I am grateful to my wife who have been so understanding and supportive, who gave me encouragement especially in times when I felt like giving up.

Project Abstract

Aim/Background: Bring Your Own Device (BYOD) as an idea exists for a long time. Now, BYOD is being acknowledged and some technologies have been developed to cope with this phenomenon. This thesis aims to point out the risks associated with BYOD, the economic impacts, the current state of the technologies used by BYOD, the challenges that face the IT departments of companies which adopt BYOD, the trends concerning this phenomenon and the scope of such idea by identifying current state as well as what would be the sustainable future of BYOD.

Method: State-of-the-art, extensive literature review was done to collect the secondary information of the BYOD technologies. As a part of primary data collection, an interview session was organized with CISCO and UNDP, a BYOD case study was done from the gathered information. The evaluation of the information was aimed to address the research question.

Result: After accessing the primary and secondary information, SWOT analysis, security analysis, threat model, and cost effects was done. The statistics show that the companies that are considering adopting BYOD is on the rise and these company's IT department would face some challenges along with it. Despite of existing security challenges, the concept has a huge interest from both customers and the companies. The concept appears to be efficient, cost-effective in long term result and user-friendly.

Conclusion: The BYOD has a huge potential however; the implementation seems challenging in respect to security issues. The increasing interests in corporate level and in user level indicate the sustainable future. The employee's productivity and flexibility, user-friendliness fosters the idea of sustainability.

List of Figures

List of Tables

Glossary and Acronyms

BYOD	Bring Your Own Device
AD	Active Directory
CASB	Cloud Access Security Brokers
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CYOD	Choose Your Own Device
DRM	Digital Right Management
EFSS	Enterprise File Sync and Share
EMM	Enterprise Mobile Management
ERP	Enterprise Resource Planning
ESG	Enterprise Strategy Group
IBSG	Internet Business Solutions Group
ICTE	Innovation Communication Technology and Entrepreneurship
IPC	Inter Process Communication
ISO	International Standardization Organization
MAM	Mobile Application Management
MDM	Mobile Device Management
MIM	Mobile Information Management
NAC	Network Access Control
NIST	National Institute of Standards and Technology
OS	Operating System
OSI	Open System Interconnection
PC	Personal Computer
QR	Quick Response
ROI	Return of Investment
SaaS	Software as a Service
TPM	Trusted Platform Model
UNDP	United Nation Development Programme

Contents

Chapter 1

1. Introduction

1.1. Orientation of the study

Recently, BYOD or Bring Your Own Device become the most popular model for enterprises to provide flexibility for users because the business environment is demanding to provide more flexible work approaches for employees[1] supported by empowered mobile devices. Expanding mobile applications' ecosystem, workers request to access business applications and companies' data from anywhere at any time by employees from any device is being demanded now. In response, organizations are looking for a model approach and a solution to support workers by using BYOD to work on their own way [2].

The term BYOD (Bring Your Own Device) collectively refers to the related technologies, concepts, policies, and strategies where the employees can access corporate data of the company and internal IT resources such as database and applications, using their personal mobile devices like the smart phones, the laptop computers and the tablet PCs[3]. BYOD concept in enterprise environment is increasing due to the mutual benefits that the company and the employees get[4]. Organizations benefit from increased productivity and reduced IT expenditure whereas, the employees can use the mobile device, which is comfortable and convenient for them. However, BYOD deployment brings serious security and privacy concerns. For example, unmanaged mobile devices and the applications installed on it are vulnerable and it might be compromised then leak the confidential data to unauthorized people[5][6].

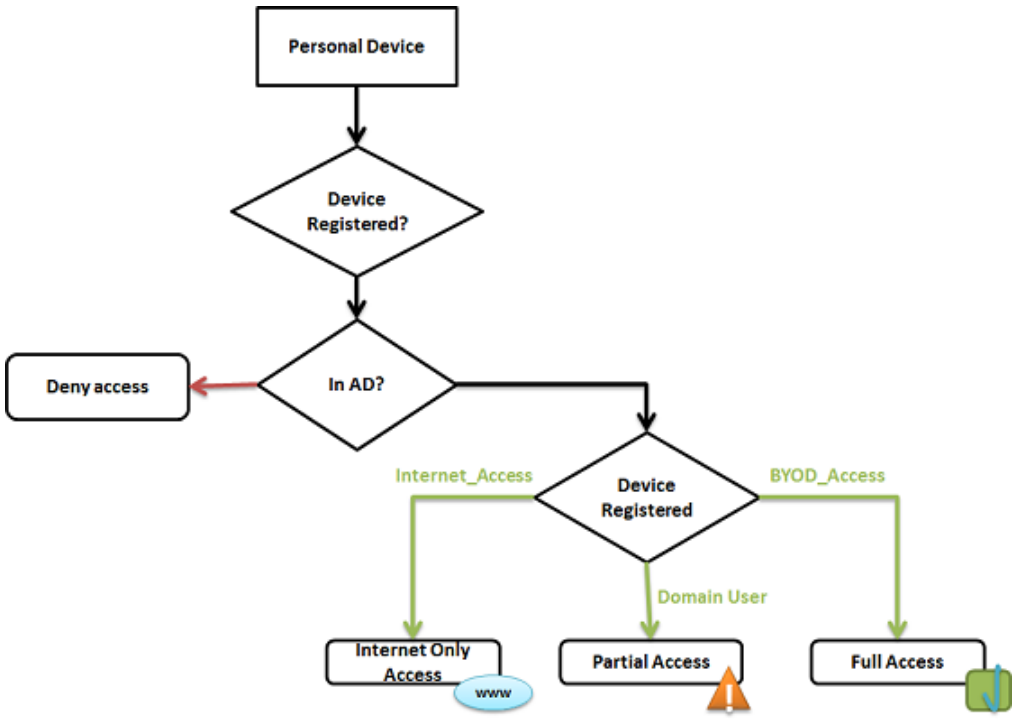


Figure 1 Connectivity Flow for Personal Devices [6]

The figure shows the different privilege levels of the device in BOYD environment

The above figure illustrates BYOD's environment in which organizations provide different accesses to network resources to their employees. Basically, all accesses (Full, Partial, and Internet only) can have access to the Internet through the Organizations network, and Full Access belong to the BYOD access active directory group which can have entirely access to all corporate resources to the network, but Partial Access belongs to domain users' active directory group which can have access to some corporate applications with boundary. There is also deny option to the specific type of mobile devices from accessing the network [6].

Critical information of organizations can be leaked if proper measures are not taken into consideration before adopting BYOD. Moreover, if due to BYOD model, customers' data get lost or compromised then the company's reputation and trust relationship might get damaged[4].The omnipresence of personal devices is changing the corporate world but, adopting BYOD comes with a set of challenges

for the IT organizations. Many of the benefits of BYOD, such as having the choice of any device and anywhere, anytime access, are somewhat antithetical to traditional IT requirements for security and support [6]. On the other hand, BYOD has an economic impact such as operational costs (accounting fees, license fees, suppliers, utilities, and devices maintenance and repairs) within the company. These challenges and impacts make companies, organizations and enterprises to enquire a risk management to define the consequences and determine the cost relations [7].

Despite all the hype about BYOD, there are hidden costs and security risks that must be considered before adopting BYOD. A common misconception about BYOD adaption is that a company can save the money by having employees purchasing their own device, but recent data prove on the contrary, which shows that it could actually be more expensive [6]. The most important points in using BYOD is that, the device owners' data will not be viewed or erased or corrupted by Enterprise actions, and they will be allowed to execute the apps they choose on the devices, and detached from the Enterprise at any time without losing personal data [8]. But for organization or information owners are important to trust the devices to access Enterprise services and data, and secure the confidentiality, integrity of the data on the devices, and be able to terminate access to their information at any time [8].

1.2. Motivation and Background

The motivation is to revolutionize or reform the use of BYOD by organizations. I am looking to discuss two points; 1) should organizations embrace BYOD? or should they hold back for the sake of their business? And 2) Research about the current status of technology used by BYOD, the security challenges that companies will face by adopting this technology and the risks it will bring to the companies and organizations by adopting BYOD.

Even though the idea was there for a long time, it's not that long since people bring their laptop and mobile phones to their work place to use for the market purpose. However, using the term of BYOD as a name only started in 2009. In the beginning, BYOD was

adapted by a few companies in 2011. Consequently, it has a huge popularity now; a survey conducted by Cisco in 2012 on 600 companies reveals that 95% of the surveyed companies are already permitting the use of personally owned smart devices in their work environments. It is predicted that about half of all businesses will introduce a BYOD environment by 2017[6].

Mobility offers new ways for user's devices and data to be compromised, according to Cisco security report in 2014[9] there are two things that appear to be helping criminals gain an edge. First, is the maturation of mobile platforms; Cisco security experts note that the more smartphones, tablets, and other devices perform like traditional desktop and laptop computers, the easier it is to design malware for them. Second, is the growing use of mobile apps; when users download mobile apps, they're essentially putting a lightweight client on the endpoint that downloads the code. Another challenge is the negligence of many users downloading mobile apps regularly without any thought of security [9].

Since BYOD is an additional enterprise endpoint, which is not owned or managed by the organization, enterprises needs to plan for the protection of these devices as an integral part of their overall endpoint, server, and security functional area strategy [10]. Bring Your Own Device as a phenomenon is so attractive for the organizations by saving money that was used for buying devices for the employees. But the security issues made the organizations to keep a distance on this solution until now; at the same time those issues presented above earlier and some other economic expenditure related to this solution make BYOD program more expensive (Cisco research).

Companies sometimes only look at the cost of the device but when you look at the bigger picture of BYOD, it is more expensive from what was initially projected, and there are several risks associated with it because this phenomenon is not yet well understood [11]. But the consequence and benefit of use BYOD will promote new business models, attract and retain talent, improve productivity, collaboration, and customer experience [12].

1.3. Research Aim

The purpose of this study is to analyze usage of BYOD concerns to the security risks and economic impacts to the organizations. This research will look for the answer of the two questions which is, should organizations embrace BYOD or should they hold back for the sake of their business. This research is based on the gathering of data related to security risks and economic impact of Bring Your Own Device as research questions which will be stated under problem definition in this chapter. Furthermore, it is within researcher's intention to work and make thorough analysis with the existing BYOD technologies. This research will also fulfill the academic curriculum for a master thesis.

1.4. History

Early in the morning after having shower and breakfast, it became a routine life for employees when they go to work to bring their laptop and smartphone to the workplace and after work time they close their smart devices (laptop at most) to bring their undone task and finish it while on their way home on the train or buses and basically complete the task at home to be ready for the next set of tasks the next day, this is a real time routine for a lot of employees' as the result of BYOD solution[3] [13].

In 2009, BYOD was first introduced and it was its first full year. It became more mainstream in 2010. In 2010, the CIOs (Chief Information Officer) have started to be under pressure by flooded devices at the workplace: At the same time Android started to follow, and that year iPad came to the market. This influx of new devices made employees bring their smart devices to work without IT supports which leads to some businesses blocking personal devices from their network.

In 2010, there were a lot of MDM (Mobile Device Management) companies' startup and iOS4 was released that year to provide first API's to manage mobile devices. Bringing own devices for work now started to be the trend which IT company and organizations realize that they can no longer ignore BYOD [13].

In 2012, the challenge of securing devices started for IT's because of data leakage and security and users were becoming concerned about their privacy. In this year, businesses

focused on BYOD policies to concerned users while they are still thinking about privacy and security implication that's why MDM solution became very popular [13].

In 2013, apps and security was a hot topic of BYOD, organizations were searching for securing devices to manage the apps and data. The mass adoption of BYOD smart devices required a management platform, which they expand from MDM to MAM (Mobile Application Management).

In 2014, BYOD started to evolve; it goes beyond email, employees expect full access to workplace on their mobile devices. MDM and MAM shifted to EMM (Enterprise Mobile Management), as industries used the capability of mobile devices for the enterprise based on used cases across user, devices, apps and content.

1.5. Problem Definition

The fundamental problem is, nowadays, the employees own multiple mobile devices such as: laptop computers, smart phones, tablets and demand for mobility on their devices. The Organizations' employees bring their privately-owned devices to work, access various mobile applications for personal and corporate use. Subsequently, the consumerization of IT extends the reach of the companies wired and wireless information infrastructure. Therefore, the personal devices operate outside of the company's IT architecture by doing so the company information also becomes more vulnerable to security breaches outside the perimeter.

The thesis will explain the usage of BYOD, as we mentioned above BYOD is focusing on remote access with mobile devices which allow employees to access information resources wherever they are and whenever they need. If sensitive data stored on poor secured mobile devices and the device is stolen or lost, an attacker might be able to gain unauthorized access to the data, and even any other data that users allowed to access from that mobile device [14],[15],[16]. Mobile devices need to support multiple security objectives: Confidentiality, integrity, and availability to achieve these objectives, mobile devices should be secure against different threats[14] [16].

Research questions:

- **What are the security risks associated with BYOD?**

There are many threats following client mobile devices to leak the confidential data to unauthorized people, including malware, unsecure networks, malicious, data security, lost or stolen devices, fired or contractor employees, etc. in this document, I am going to research about those risks associating with BYOD when organizations considering to adopt this trend.

Sub questions:

- **What is the current status of technology for BYOD?**

To focus on mobility strategies and company policies, we should focus and look at the current technology that exists related to BYOD. The technologies and tools are available now are evolved, we can see the evolutions when we look at the current state of the technologies. When the company talks about BYOD, they are thinking about Mobile Device Management (MDM), and when they think about that MDM is so restrictive, then they moved to Mobile Application Management, and now we are moving to Enterprise Mobility Management. So, that's why we need to look at the mobility management tools, and we must look at the user's experiences in implementing things like responsive design.

- **What are the market trends of BYOD?**

Rise in productivity of the organizations lead to BYOD adoptions across varied companies; this ultimately helps the market to grow at a rapid pace. Increasing employees demand to use their own devices at work and the popularity of remote accessing and existing security solutions for allowing remote management of mobile devices plays an important role in supporting the use of employee's own devices at their work place.

- **What are the challenges to IT department for adopting BYOD?**

The way we live and work is changing fast, users are now becoming innovators, consumerism is driving changes, that's why there are challenges to the IT department of the companies that are adopting BYOD; to make sure the data ends on the devices are secure and the communications between client devices and servers are secure which means to enable users work how, when, and where they want.

- **What are the reflections of costs by adopting BYOD on the organization (Cost Efficiency& Impact)?**

In relation to the benefits of BYOD to the employers, there's the reduced device and technology costs, the advantage of newer devices' upgrade to latest hardware more frequently, and improving user's productivity and satisfaction by using their own devices. On the other hand, there are some hidden costs such as helpdesk, license, user's subscriptions and connectivity. These are the costs which are related to BYOD, on both ways (spend and save money) that need to focused on before adopting BYOD.

1.6. Limitations and Delimitations of the study

This study will cover the analysis on current usage level of BYOD, try to identify, assess, and analyze the security risks as the effect of uncertainty on the objectives followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. This security risk management will assure the uncertainty about BYOD, and organizations will not deflect the endeavor from the business goals.

There are advantages and disadvantages of BYOD security, which the author will research on and provide the state of the art. A brief historical, current and future situation of BYOD is provided. The study is limited to the technical aspect, there is not a real product, nor any conceptual products that are developed but only an estimation of what will be the risks associated with BYOD if companies decided to adopt the system and its state of the art, the abstract and analysis will be the conclusion of this report.

1.7. Chapter Conclusion

The first chapter introduced the whole project concept followed by the motivation of the project and the brief history of BYOD. This chapter also defined the project limitations and introduced the research question. This chapter, in general, is the introduction to the research idea, formulating of the research question and the motivation of the author in this area of interest.

1.8. Outline of the Thesis

Chapter 1: Introduction

This chapter focuses on the discussion of the background of the study, the problem statement, the research questions, and the science involved, if any, of the study. The chapter provides an overview of the general background of the study and ends with a summary to prepare the reader for the coming chapter.

Chapter 2: Research Methodology

The chapter presents the approaches and methodology used in the research that include the research approach, the research design, data collection, data analysis and ethical considerations. Finally, a chapter summary rounds off and prepares the reader to the next chapter.

Chapter 3: Literature Review

The chapter presents a literature review of BYOD security, the challenges, security risks, economic impact, and the trend of BYOD on what other authors discussed and tackled issues that are related to the study. It provides conceptual background on the topic studied and prepares the reader to the next chapter.

Chapter 4: State of the Art

This chapter presents the current state of the art technology that exists in using BYOD and points out of the reason of having different forms of device management on different

level. A chapter will end with chapter conclusion and prepares the reader to the next chapter.

Chapter 5: Case Study& Interviews

This chapter will present a practical case study by conducting organizations interview, and some BYOD illustrations based on organizations interview. The chapter will end with a conclusion and prepares the reader to the next chapter.

Chapter 6: Theory and Considerations

The chapter presents the theory and some considerations which will be use in the research to support the author to find a practical answer to the research questions. It provides 11 functional areas of Enterprise Cybersecurity, and SWOT analysis in theoretical manner. A chapter summary rounds off and prepares the reader to the next chapter

Chapter 7: Research Analysis

The result of the study is presented in this chapter. It includes the validity and reliability of the result, different objectives and opinions of the result are also discussed in this chapter. It prepares the reader for the next chapter.

Chapter 8: Discussion and Conclusion

The chapter discusses the research findings and links them with literature review where applicable, it also presents conclusion drawn from findings.

Chapter 2

2. Methodology

2.1 Research Methodology

This chapter presents the steps, methods, techniques and tools that were used during the research of this project. The methodology provides systematic and logical steps to serve as a guide and provide direction in answering the research questions. The methods include; primary data which is arranging an interview with different companies which have been implementing and not implementing BYOD; the secondary data is analysis, which is the use of existing sources (such as official statements, papers submitted to public consultations and news sources) and approaching the pages related to the subject and the technologies.

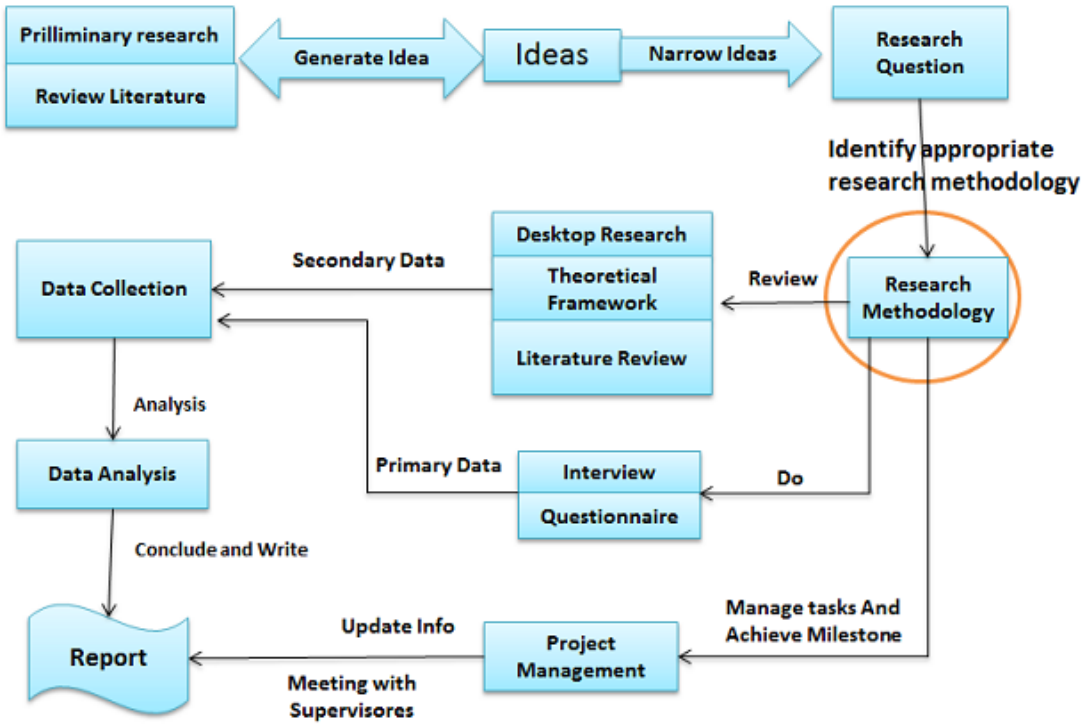


Figure 2: Process Overview (Author)

The figure depicts visual representation of the whole research process from the very beginning step: the preliminary research, to the final step: the report submission step.

The main steps of the project process are discussed below.

2.2 Problem Formulation

In the very beginning of the project, preliminary research and desktop research was done to intensify the brainstorming process to generate ideas. Set of ideas were generated and presented to the supervisor. Among the ideas, BYOD was chosen as the topic of the research during the constricted process of meeting with the supervisor. The topic was further discussed and refined with the supervisor to develop it as the research question, which is mentioned under the **problem definition** section.

2.3 Data Collection

Once the problem definition was established it was time to develop the methodology, where the first step was to review the existing adopted BYOD solution. This could provide an insight to look at the problem from the different angles. This step was about trying different ways to collect the data related to the research question. The collected data was then analyzed from the desktop research, the questionnaire technique and interview method to collect primary data from the companies which have adapted BYOD and those which have not adapted BYOD. The analysis chapter includes the summary of the primary data collected through interviews and the detailed part is included in the Appendices.

- Primary Data

There are different methods of collecting data from users, like questionnaires, web-surveys etc. but some people prefer to be interviewed, especially if the interview topic is interesting and relevant to them, so they do not have to spend time to write anything down. If participants are interested in receiving feedback, then this situation also provides that opportunity. Interviews are inductive and are open to give the opinion but questionnaires are close and more appropriate for quantitative data collections. I prefer interviews rather than other data collection methods if it is possible. Primary data is called as such because it is a data taken directly from the primary source, i.e. the person being

interviewed or surveyed. According to Mark Saunders, personal interviews achieve a higher response rate than questionnaires [17]. In another “article, “Steinar Kvale” also write that there are not fixed rules for interviewing but different techniques can be used through the process of an interview to produce knowledge. Interviews can help to discuss in the areas where it has direct relation to the research question. It also gives interviewees the opportunity to ‘think aloud’ and discover something new [18]. I approached different companies’ IT department by calling them or sending them an email to ask them for interview to collect data related to the security risks associated with BYOD and the economic impact. I also asked employees as a main part of this adoption if they are ready to buy their own device and use it for their work and give the permission to the company’s IT department in taking control over their devices.

- Secondary Data

Secondary research data is also known as a desktop research (Literature Review) refers to seeking facts, general information on a topic, historical background, study results, etc., that have been published or exist in public documents. This information can be obtained from libraries, newspaper archives, government, university, and websites. The book ‘Research Method for Business’ also explains the importance and the requirement of the secondary data. Chapter 8 of the book ‘Using Secondary Data’ summarizes that most research projects require some combination of secondary and primary data to answer the research question(s) and to meet the objectives [17].

2.4 Data Analysis

The knowledge, information and the data collected from both primary and secondary sources become the input to make an analysis of the research. The basis for the secondary data source are the state-of the-art (chapter: 4), Case study and Interviews (chapter: 6) and Theory and Considerations (chapter: 5) and Literature Review (chapter 3).

2.5 Project Management

Project management is the timetable of workflow to restrict researcher with plan and the progress of project within the time that has been planned for it. To create timetable of the project, a simple Gantt chart was used. It was quite simple and straight forward way for presenting the initial project planning and the phases. More details of time table are included in the appendix 1.

2.6 Tools

The different research materials were studied to deeply understand the current state-of-the-art of the BYOD. Most of such reading materials include IEEE's published research papers and white papers etc. Many white papers from the main Enterprises, as a market player in BYOD market have also enriched the research.

SWOT analysis: SWOT analysis is a tool for strategy planning; it helps an organization to better understand the internal and external business environment to make a strategy plan and decision [19]. It's important to identify the strong point of the business idea and make it even stronger and as well as define the weak point of it to make them stronger, and then define the threats to be protected from it. In any kind of business, there are some opportunities which should be worked on and benefited upon in order to develop the business idea and strategy [20].

The 11 functional areas of enterprise Cybersecurity: 11 functional areas are one of the frameworks to analyze major trends impacting how enterprises think about their own IT and security. Even though there are plenty of different types of frameworks such as (ISO 27001/27002 Version 2013, NIST cybersecurity Framework (2014), etc.), all of them are excellent framework for running an enterprise's cyber security program. However, a good framework alone is not going to stop cyber attackers who are targeting an enterprise and attempting to defeat its cyber-defenses. Well-organized Cyber security capabilities are not going to protect an enterprise from advanced attacks all by themselves. To be effective, those capabilities have to be applied in ways that disrupt, detect, delay, and defeat targeted cyber-attacks[10].

I chose 11 functional areas of cyber security framework as a methodology to do research because I am familiar with this framework from my previous semester subject (Cybersecurity and Trust) which is exceptionally relevant to bring your own device in the sense that BYOD is a tool for modern enterprise system to be used by their employees. I was impressed with that subject and it has been well documented in the Enterprise Cybersecurity book which is to analyze BYOD security system.

Literature Review: A literature review has been used to present the current knowledge available that is relevant to the study aim and research questions outlined by the author. This is a crucial element of the research, for almost all researches to review a relevant literature and compare with other related studies. Literature review is used to introduce different description of BYOD and then discussion trends and usage of BYOD in the organization and Enterprises, and the benefit of BYOD usage in the organizations and business environment.

2.7 Chapter Conclusion

This chapter introduced the process of working in this research project. It started with the explanation of where the idea came from and how to collect the data and information for the research. The methodology as the process of the project on how it would be managed and the timetable of the work has been defined. Timetable has been followed as was initially planned but due to the period of summer holiday in Denmark, the author couldn't arrange company's interviews (IBM, MobileIron for example they couldn't accept the Interview requests since their related workers were on holiday) to collect more practical data (primary data) for the research.

In relation to my thesis quality, I must revise my thesis to fulfill the requirements of my master thesis in a satisfactory manner. That's why this thesis project report has been added 8 weeks more which is why it will be hand in date (15-11-2016) in order to be revised. Time table of the revise schedule is located on Appendix 2. In the next chapter, I will focus on the Literature Review of my thesis.

Chapter 3

3. Literature Review

The Literature review presents the current knowledge available which is relevant to the study aim and research questions outlined in chapter one. A crucial element of all research is the review of relevant literatures to compare with other related studies. Hence, this chapter represents review of the literature of the existing system. It was important to understand the theory and the state of the research in problem related technology and existing solutions. This chapter firstly introduces the different descriptions of BYOD then, discusses the trend and the usage of BYOD in the organizations and the benefit of BYOD in business environment and the risks this phenomenon will bring to the organizations.

3.1 Concept of BYOD

Many professionals have more than one mobile device with them or in their pockets: one for business purpose and one for personal use. While some have more than one for entirely other reasons. All these devices have different passwords, settings, data sets, configurations, and so on. These multiple devices with multiple configurations and different OS's will bring complexity and confusion to the user and to the system corporation as well. Nowadays, wireless mobility covers a big part of our daily communication, most of organizations facilitate to its members by providing a structure to allow them to use their own device to connect and use organization's network resources [21]. Technically, it is possible to collect the functionality of all devices into one device if the users are willing to use their own devices for both work/business and home/private use [22] the concept that is able to do this job is BYOD phenomenon. The main idea about Bring Your Own Device is an enterprise and organizations that set up an IT strategy to let people bring their own device to work. This initiative focuses on programs, policies and strategy; the concept gives freedom to the user to use their own device. Based on technology foundation of enterprise mobility management, BYOD has proven best practiced in enabling organizations to empower people to improve productivity and

collaboration [7]. In brief, we can use BYOD term when members of an organization are allowed to use their own devices while connected to the organization's network and can access to the organization's data [21].

Cisco[6] describe BYOD as: an idea where end users are able to use the computer and communication devices of their choice, to increase productivity and mobility, those devices can be purchased by employer, or employee, or both. BYOD means any device, with any ownership, used anywhere at any time. However, enterprises for cloud service solutions [23] describe BYOD as: a policy to define how individual employees can bring and use their own personal devices, e.g. laptops, tablets, and smartphones, in the workplaces. Accordingly, they said [23] smartphone BYOD is particularly more desirable for the enterprise because it assists new trend in the workplace by connecting people in all places. (EunByolKoh, Joohyung Oh, and ChaeteIm) in their document describes BYOD as a collective of related technologies, concepts, and policies, where employees do work accessing corporates internal IT resources, like database and applications, using their personal devices such as smartphones, laptop computers, and tablets [24]. But Ognjen Krstulovic from UNDP department in Bosnia-Herzegovinian define BYOD in two ways; one is, company's policies and attitude to allowing the staffs to use their own computers for work, and providing the organization to use their equipment at the office or home; second is user managed devices used for work which company is not responsible for managing the devices [UNDP Interview]. But UKSime has a different description to BYOD, it says that it is using techniques and abstraction mechanisms to deliver applications to end users at any time and in any device style [21]. The following figure will illustrate this concept.

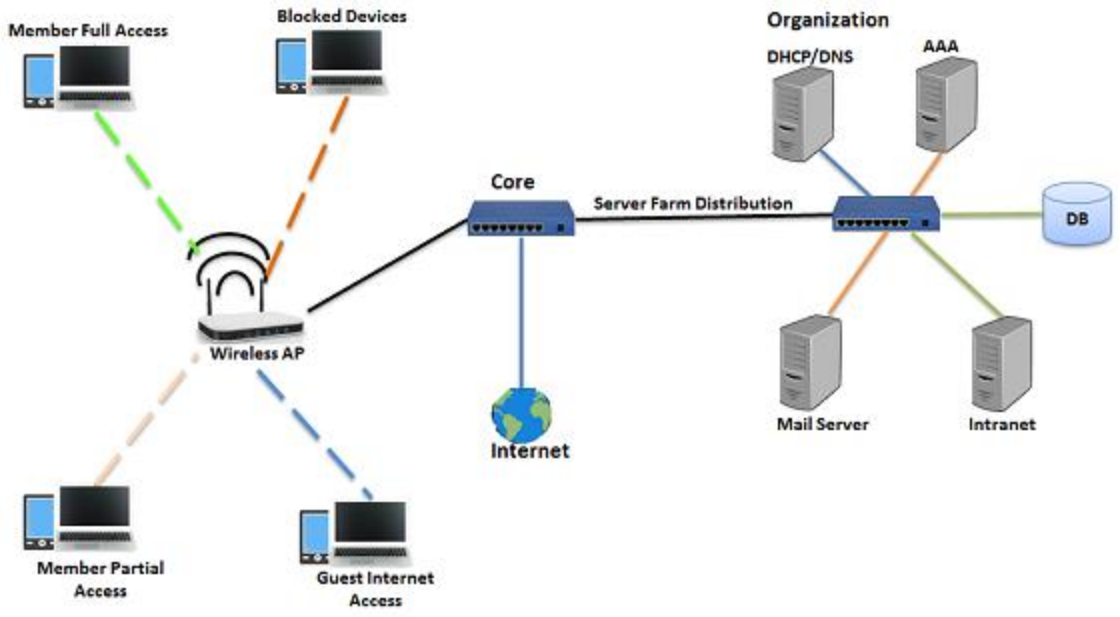


Figure 3 Simple Logical BYOD Topology [21]

This figure depicts the simple logical topology of the BYOD

The figure above illustrates a simple topology of using BYOD. There are two options as the base: the device can get an access or the device can be denied to have an access. In the case of access denied, it is the end of the scenario without having any access, but in the case of getting access their will be three possibilities, and this is the idea behind the BYOD phenomenon.

1- Members full access: The employee will have a full access to the Internet and to the organizations corporate data even sensitives data and applications which can change and retrieve data with respect to the privileges and policies.
2- Members Partial access: The employee can access to the Internet and some applications (Limited access).
3- Guest Internet Access: The employee will have only the access to the Internet.

BYOD is already existing and implemented in many businesses [25], even though there are different abstract and opinions about what BYOD is as mentioned above, most of researchers and the organizations believe that, if BYOD can be used properly it will certainly bring benefit to the companies in term of improving efficiency and cost reduction [25][24][23]. For example, in [24] says the businesses are actively adopting BYOD in

order to improve their productivity and reduce the cost of device purchasing. And [23] stated that enterprise benefits from BYOD by reducing the operational costs by shifting devices cost policy to the users. Consequently, BYOD will bring extra security risks to the organizations, such as, vulnerability, malicious attacks, data leakage, data breaches, device being compromised, and device lost or stolen with company's confidential data [26]. Therefore, when companies and enterprise are adopting BYOD, they should consider how to handle sensitive data and protect their data from malicious and Internet criminals while the data is on transition or on the rest on mobile devices.

Nevertheless, each organization might have different key drivers of using mobility device which depends on the nature of their business. But they add this to utilize mobile applications to drive productivity gains, sale performance, reduce cost, customer and employee's satisfaction [27]. Moreover, organizations can facilitate the acceleration of business processes by using BYOD and provide more flexibility to workflow, improving response time, communication, collaboration, and reducing operational cost [28][27] [3]. On the contrary, with these new opportunities come a bunch of challenges such as device selections, applications management, device manageability, access control, security, and connectivity [3]. These are the challenges of organizations' IT department, to meet the usage and benefit of the evolution of mobile devices capabilities. Forrester [29] reported that the main concern about BYOD (employees mobility) is related to the security in the particular device, data breach, an application securities, and data mobility which consequently increases the risks of unauthorized contact to sensitive critical data. It also create many challenges for organizations' IT division in ensuring information security and in controlling the use of technologies [29].

All the above-mentioned description and different opinions are about employees bringing their own device. Based on their definitions and description, BYOD is the choice of employees to use their own devices for work purpose and having an access to the company's internal network seamlessly at any time and from any were with any kind of devices. This choice is technically possible, and by designing and implementing a proper strategy and policy it's possible to save some costs within companies by using this phenomenon (more cost detail in section 3.4). But if the organization is not aware to build

some good policies based on some strategies, then the company will fail to fulfill the purpose and goal of BYOD. This phenomenon will bring some risks and challenges to the company that's why organizations must be consider to these two questions; why the company want to adopt BYOD? and how they plan to adopt BYOD?

BYOD has different purposes such as employee's satisfaction and productivity, improvement and collaboration, and removing the boundary of employees working only within office premises. Some companies must adopt BYOD because they may lose the competition to their similar businesses that use BYOD which results more customer/employee's satisfaction, employees' productivity and fast response to the customers.

Based on the above-mentioned from different researcher and literatures, in the following sections I will point out some benefit and challenges of BYOD to the organizations.

3.2 Benefits and Challenges of BYOD

Through BYOD existence and the above views, there is a clear proof of the benefits of this phenomenon. BYOD is a system that allows and facilitates communication within the company and company can use mobility's applications, wireless technology to enable communication, and information access, as well as business transactions from any device, from any were, from anyone, at any time. Enterprises can use BYOD by providing integrated applications architecture to enable employees to access corporate resources by company provided and privately own devices at any time. This integration architecture will allow employees to serve customers better. Bottom line is the benefit of BYOD is integration, customers/employee's satisfaction, availability, productivity, improved adaptability, access remotely, mobility, flexibility [30], and mobile applications & devices presents new opportunity to the organizations to communicate with their customers, partners and suppliers. Basole [31] observed that the point of Mobility solutions, such as mobile email, dominantly on basic communication and productivity improvements. Consequently, BYOD trend will promote new business models, reduce cost (more details in section 3.5), attract and retain talented people, improve productivity, collaboration, and customer experience.

And to elaborate more, there are several challenges in adopting BYOD in general and specifically concerning to the security, that's why the deployment of this platform should be done in a proper way with the use of a suitable technology for different purposes. One of the biggest challenge for organizations is that corporate data which is being delivered to devices are not managed by the IT department which has security implications for data leakage, data theft and regulatory compliance [32], because with unmanaged devices, organizations have less control and visibility, and fewer mitigation options than they do with managed devices. A survey shows that 88% of IT directors believe the employee's morale is improved with an organization's BYOD policy [11]. However, in another survey [11] 75% of IT managers are concerned that BYOD will increase security issues in the organizations from allowing consumer focused mobile devices in the office, this will create direct implications on security, information ownership, device/network control, and even helpdesk resources. The security challenge would be who and what is on the network, having malware free network, what kind of information can be stored on the endpoint device, enforcing access policy, and auditing the requirements.

PWC in their service advice report [12] state that to implement and enforce a very strong set of policies to govern employees to bring their own device and access would challenge of IT administrator because the weakest link of mobile device security is often the user, and policies should be designed very carefully to meet the need of users and safeguard the organizations data according to the organizations business model.

Cisco in its whitepaper about BYOD [6] says, to understand the challenges BYOD pose, we should understand the business trend that are driving BYOD adoptions, Cisco dividing the challenges in two categories, IT organizations and challenges for end users. The challenges for IT would be, IT should support to provide device choices, the IT must approach BYOD's problems differently from the traditional IT pre-determined list of approved workplace devices because devices are evolving rapidly, it is not practical to determine and pre-approve each device brand and form factor. Maintaining secure access to the corporate network, device choice doesn't mean to sacrificing security, IT must establish minimum security requirement to any device must meet on the corporate network [6], and on-boarding of new devices which means bringing new device on to the

network for the first time should be simple and easy and ideally self-service with minimum IT intervention: enforcing company usage policies, visibility of devices on the network and protecting data and loss prevention. One of the largest challenges with any BYOD implementation is ensuring data protection with corporate asset. Cisco and (Wang & Wei in their document [33]) have the same opinion in revoking access, it is needed because, at some point the lifecycle of device or employee and device lost or stolen, it will be necessary to terminate access to the devices. IT needs the ability to quickly revoke the access granted and possibly remotely wipe data and applications on the device. The challenges for the IT department are; to keep it simple solution so users can follow the steps easily to get connected and use corporate resources; separate user's private data from work data which it calls mixing personal device with work such as contact lists, E-mail, data files, applications, and internet access this can be a challenge [6]. But [34] looking for the points of how BYOD can be useful as a challenge, if it is necessary to deploy it and why? Because as mentioned before BYOD adaption will bring a lot of risks and challenges, so the organizations should analyze and determine the benefit and cost of adaption.

This involves analyzing all departments and identifying employees' responsibilities and roles, which technology can be used to fulfill the purpose and differentiate the data in the sense of which can be accessed and which not by mobile devices by sensitivity. Basically, the organization should answer the following questions to challenge the deployment of BYOD. And at the same time [34],[33] considers that different operating system supporting clash is one of the issues and challenges because they need an equal support, and the other challenge is employees' reactions, emotions and observance of BYOD security policies. The policies need to show the employees handling situation when he shows resistance, and observing mobile devices used for illegal activities, and employees lack of security awareness [33]. Employee Training- teaching staffs in the way they understand and follow BYOD policies is an issue, the challenge will occur when you need all staffs to have the same understanding of companywide BYOD security policies, because the main goal of training is to make user accept the device in use, ensure awareness of risks and maintain good security practices [34][6].

Technical challenge is a primary concern of security challenges in BYOD deployment this challenge has several aspects:

Access Control is one of technical challenges that will be phased in adopting BYOD, Sara Ali in her document [4] explains that organizations determine the access controls based on two models; some access control models provide access by analyzing attributes of device while the others are dependent on employee's profile, the organizations should be very concerned for the given permissions while being aware who is doing what, Figure 4, sometimes some employees will connect to another company by the same device. And [34] says, companies should determine and control access time limitations, how many people can access the same document at the same time, how employees gain access to the company's resources of course, these depend on company's size, location, number of employees and so on. But in my Skype interview with UNDP department in Bosnia-Hercegovina Ognjen Krstulovic said, with his 20 years' experience in the ICT unit in the department, this kind of issues can be solved by designing and enforcing good and strong security policies (UNDP Interview), his most concern is how to motivate the users to follow the policies and use mobile device in the right way.

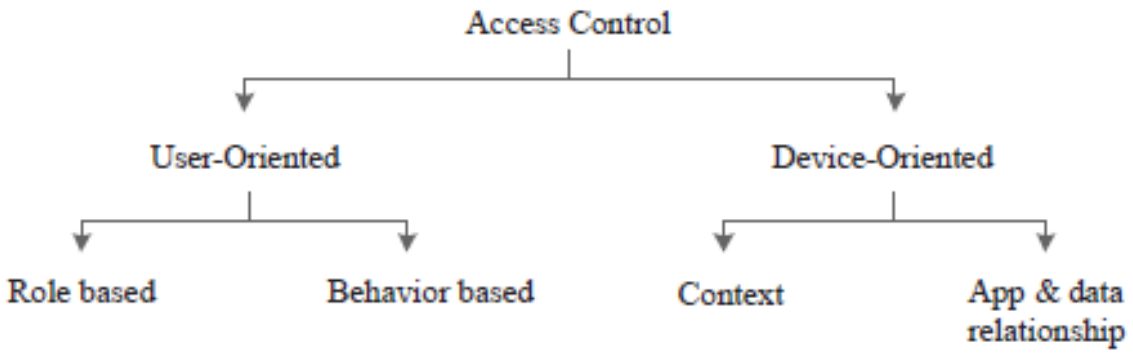


Figure 4 Access Control Model [4]

The figure depicts the access control model showing technical challenges which is one of the BYOD security challenges

Required Security Measures- adjusting security measures to unpredictable employees owned devices is not easy and a heavy strain on resources and personnel responsible for maintaining them.

Controlling data Distribution- containing, monitoring and controlling the distribution of data is a priority of organizations to maintain integrity and confidentiality of organizations' data need to be controlled because once data transferred from their network to the device, it should be monitored and it is complicated. Although, it also depends on the data transferred and stored on the mobile device or it may only be accessed [34].

Maintaining Network Connection- maintaining secure and stable connection is a challenge because mobile devices will connect via external network and it's a concern for BYOD businesses' dependency. Wireless access, unprotected WiFi hot spots are factors for threats like malware to install itself on the mobile device [34] as mentioned in the vulnerability in next section (3.3.2 and 3.3.3).

Protecting Cloud Storage- cloud protection and facility is a sensitive issue because cloud stored data applications enable data to be accessed by mobile devices, when the cloud storage has been accessed by mobile device it will be threatened by software based attacks, hacking. If the company is unable to control the transfer of data the security loop holes will be created [34].

Remotely wiping data on the devices is one of another technical challenge, because the devices are used for both personal and work purpose, and it is a final decision/solution of the security on the device [15]. When the device is lost or stolen, and even when the device is defect or retired (life cycle), and in the case of contractor employees, employee fired or any reasons of user's separation from company, there must be a mechanism to remove company's data from the deice without affecting users' private data. This mechanism is related to the policies and administrative operation [35] corporate data and applications should be logically separated from personal data and applications [36] One of the challenge for instance, in the interview with UNDP department interview in Denmark with (Moe kyew global ICT specialist & global connectivity support on UNDP head quarter) he said, "one time the malicious attacker took control over one of our laptop and

he demanded money to release it, but because there were not so important nor sensitive data in it and we had a backup, we just reset the computer totally." And another case in the other UNDP in Bosnia-Herzegovina Ognjen Krstulovic said, one of their devices has been lost, but before they wipe the data from the device they have been changing the permeation control of the device, that's why they were not capable to wipe the devices applications and data. Remote wiping is an incidence response [10] it is the final reactive solution that is triggered when one of the above-mentioned situation occurs like lost or users separate from the company [34][37]. This is an incidence response for the system to wipe and rebuild. However, in US the regulations give right to the organizations to monitor and wipe the users' device [37].

3.3 The Security Issues

Employees own devices are typically perceived as less secure than devices issued by organizations [38] this is because of two reasons, one is because employee devices cannot be controlled and exercised by the companies as it can do on company owned devices. The control is not only authentication, encryption, secure connection, network, etc. but the choice of platform and manufacturers are also a big security issue. And second, employees are using their own device for both private and work related activities, resulting of both activities corporate and private data accessed and stored on the same device. Therefore, employees owned device may pose greater threats and vulnerabilities against corporate assets, and it is easier to become compromised than device owned by company [38]. However,[11] point out that BYOD is expected to increase security issues for organizations because BYOD means supporting different kind of devices with variety of OS and maintaining an expected level of service. The effect of granting accesses to different personal devices has direct implications on security, information ownership, device/network control and even helpdesk resources. In addition [25] states that when an employee attaches a personal device to an organizations network or machine the organizations should be worried about overall security because, as soon as personal devices are attached to companies machines and over companies network the malware from devices can migrate to the company's machine or network. And on the other direction a sensitive data is possible to be leaked from the personal device when it

remained and saved on the devices. That's why when this kind of information leaked out from devices bad thing can happen, especially if the device is lost or stolen [25].

There are four enterprise mobility scenarios which vary in their suitability to handle sensitive data [30].

1. Corporate unmanaged arbitrary device model and OS to access Internet through organizations' network.
2. Corporate unmanaged arbitrary device model and OS to access non-sensitive data from the organizations.
3. Corporate approval device model and OS, with corporately managed access/storage for sensitive data from organization and separating personal and work data.
4. Corporate managed and approval device model and OS, to access/storage highly sensitive data necessarily separating personal and work data.

Antonio Scarfo in his document [39] expressed, based on the research survey done by ESG (Enterprise Strategy Group) performed on 315 security professionals working for enterprise organizations, about their difficulty of security challenges for mobile devices they identified that: 48% of the challenge is enforcing security policies for the mobile devices, 46% is lost or stolen devices which containing sensitive data, 46% sensitive data confidentiality and integrity protection when accessed or stored on the mobile devices, 41% is the threat management on the mobile devices, 41% supporting new devices, 40% of the security challenges is creating security policies for mobile devices. So, the potential threats are related to the mobile devices access to the data and applications, the attacks come from the devices or from the external network, and how to protect the data.

3.3.1 Device Security

Device Security is one of the main issues for employees to bring their own device [11][25][39] and it's architecture is lack of security measures in the end device. Security issues will be any, were at the different layers including a network layer, but in the case of employees bring their own device the issue will pop up in the device layer [40]. The applications on devices can leave the companies/organizations data on the device, and if in case the device is lost or stolen there are possibilities to misuse the remained data on the device [25][26]. Furthermore, by using the same device for work and private data possibly the data will be mixed, this data mixing could cost the organization's data leakage, for example if the company's information accidently is sent to personal contacts [40].

3.3.2 Malwares

Malwares are another concern issue because mobile devices are also working as a normal computer which can be infected by malware, which tends to steal personal information from the devices [40]. The number of malicious apps (malware) will increase by increasing in number of apps on the device because some of the apps are very possible to contain malicious code or holes when the users download apps without testing from the organizations [26][37]. Mobile application Malwares may not target enterprise or organizations data directly or specifically, but it may create a breach by compromising device to create a backdoor data leakage for BYOD scenarios or to engage in denial of services [40]. Mobile malwares are apps embedded with malicious code which is trying to compromise the security of devices or related data [37] the most common type of malware on mobile devices the paid version of apps that have been released for free, these free version paid apps are embedded with codes to export sensitive data. If an attacker have a physical access to device it may install malware on device to gather information, and when the client device accessed to the system it may infect the system with malware and spread throughout the organization [15].

3.3.3 Applications

App vulnerabilities and weaknesses consist issues within custom or commercial software that may sometimes un-expectedly expose the data within the applications or assist malicious in compromising the device [37]. Most of the organizations know that allowing their employees to use their own device help them to meet their business objectives and they also recognize that their data and information faces more risks (explained on section 3.1 and 3.2). To protect and save their data from internal and external threats they need to make sure that every mobile device that is accessing their network must have appropriate security control installed [37][7]. According to Infonetics, [32] almost all the enterprise surveyed by Infonetics found or reported by users have been downloaded malicious apps on their devices. And more than 64% of devices containing organizations sensitive or proprietary data had been lost or stolen but only few of them had a protection solution on their devices [32]. Most of malware has been written to collect information on users installing different applications including games on their mobile devices that can potentially be malicious and put enterprise data to the risk; with access to the corporate data by unmanaged devices and infected by those kinds of apps, a careless employee can risk leaking information.

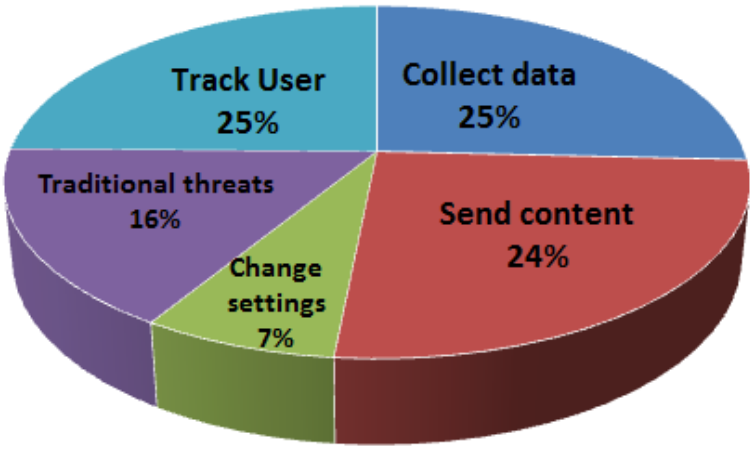


Figure 5What Mobile Malware Does with Your Phone [32]

This figure provides the answer to the question what a mobile malware does with a user's phone

Malware written for mobile devices are increasing threats, especially for Android and for jail broken iPhones, but Windows is more attractive for malware than Apple and Linux. Although, Android is attracting more number of mobile malware threats, because Android is an open source and it's easier for developer to write malicious applications. The mobile device vulnerability management is a top concern for security professionals in the next 12 to 15 years, because it's very important compared to other security initiatives [32].

3.3.4 Users/Employees

Employees or users can be one of the security issues and can also be a strong point of security, the weakest link in the mobile device security is often the user [12], but if the user follows the policies and strategy of IT administrations in relation to updating device software on time, avoid downloading unsafe applications or content, not visiting strange links and malwares, protecting account details (username, password), and participating in the instruction or information about using the system, it will be a strong point to pursue security requirements (author). It's also difficult to detect a malicious user by abnormal behaviors such as suing stolen terminal or internal data access and an internal malicious behavior [26]. Employees can easily steal company's secrets and trade secret idea, intellectual property, and sensitive information about customers. This can happen by saving that information locally or to the cloud service then further more can send it through an account to Dropbox or email it by personal webmail account [32].

Sometimes, the users are not aware of what they are doing, in the case of BYOD the personal device can be used for private purposes and can access to the public Internet, if the users are not aware it's very possible to download a malware or viruses which can affect organization's data and applications. Users lost devices, users' login in the public area can cost stolen access identity, users who are ignoring or not willing in updating software device on time, users who do not accept the terms and conditions of organization policies can compromise security. [1].

Personal devices that are used for enterprise work are becoming a part of enterprise network, so it's important that all mobile devices within enterprise network are up to date and to enforce the enterprise security policies on the personal devices[11]. But since

BYOD will bring a variety of device hardware and operating systems, the systems' security policies will change from time to time with new security threats, this will be difficult to enforce due to the constant need for updating corporate and personal devices [40].

3.4 Trends and usage of BYOD

The number of existing mobile devices increase day after day, a study by Cisco group shows the number of BYOD devices in six countries has grown 105% between 2013 and 2016 from 198 million to 405 million devices [41]. The United States currently is the largest BYOD market with 71 million devices and expected to be 108 million by 2016. In the same study, it stated that 30% of mobile device users would rather work in the environment where they allowed user to use their own device, especially in Germany, most mobile users would rather have a company-provisioned device. BYOD-ers are willing to spend their own money and even pay for their voice and data plans for their BYOD device. Productivity and flexibility also encourages companies and organizations to be more interested to adopt BYOD. It shows that the employee's productivity, flexibility, employees readiness to use their own device, and increasing the number of mobile devices will encourage the organizations to adopt BYOD. In short, BYOD is fast growing and is a strong trend today[42].

Antonio Scarfo in his document [39] about the trend of BYOD state that BYOD is now growing trend, existing several frameworks based on state of the art of telecommunication technologies, users knowledge about new technologies, existing the same functionalities of traditional computer on mobile devices, new generation converged/unified heterogeneous mobile networks, quality of service, resource reservation, admission control, policy management, employee demands, on that bases the companies are modifying their IT models. This will expect a huge number of companies shifting to employee-owned device. And another evidence that make BYOD trends and desirable is cloud computing, work-shifting, and improvement of the bandwidth availability [39].

Shifting from work on-promises to cloud based will encourage organizations and companies to adopt BYOD (interview with Moe Kyew Global ICT specialist, and manager of the global connectivity support in UNDP).

Bill Morrow says, the [32] ability to control and secure sensitive data, increase of web applications, cloud computing, and Software as a Service (SaaS) offering are trend in impacting organizations to adopt BYOD. Bill continuously defends his confidence on BYOD trends saying that, based on survey done by Harris Interactive, more than 80% of employed uses personally owned electronic device for work related function. Increasing on efficiency and flexibility by giving access to the corporate data to the employees owned device has been approved, that's why employees bring their own device trend will advance and companies don't want to be left behind in the competition [32].

3.5 BYODs Cost Effect

BYOD might come with a high initial cost, but the payoff should be worth it in the long run [40]. BYOD offers cost efficiency for organizations by putting devices purchase on the users, the employees productivity, efficiency, and satisfaction in the global scale will benefit the organizations [1] [UNDP Interview]. Samaras says, [23] enterprises will benefit to reduce the operational cost by using BYOD's cost policies, this will be achieved by shifting to the user, removing up-front costs for IT hardware and software owing to the per-user service-renting model.

In the document [7] stated that, one of the primary benefits of BYOD is cost reduction by employees readiness for paying part or full of the cost devices used for work. As mentioned before in the introduction and Cisco's interview, BYOD phenomenon is two sides benefit. On one side, users demanding to use their own device for work purpose for flexibility and concern to work at any time anywhere to access the work-related data, and the matter of not carrying multiple devices (private and business devices) and users' experience to their own devices. On the other side, the organizations can increase employees' productivity, collaborations, and customer's satisfaction. Many organizations and enterprises are concerned regarding to device cost and reducing the operational costs. This is achieved by shifting BYOD policies costs to the user such as reparations cost, device lifecycle, and device defection [23].

There are also significant hidden costs associated with BYOD adoption, which are not related to the hardware, many of these costs are tied to support, and it also depends on

the policy of company in implementing BYOD strategy and policies and the agreement between companies and employees [37] For example, international organizations should consider the capability of cellular network providing and usage of data by workers. It will increase the organizations cost if the companies are taking responsibility of the employee's bill, especially the companies with employees traveling internationally. Mitigating disruptive, security events, responsive, and cost-effective solutions are costly that's why when the company implements BYOD strategy, they must be consider to those expenditures because they are expecting higher productivity and cost reduction [43][44]. Gartner in cloud security says, [43] digital business introduce a new security risks, to manage the risks it needs the latest security technology trends to maintain effective security program which it will be costly. Organizations to enforce security policies to have a greater control over security need to provide some security devices such as, VPN gateway, firewall appliances or other security devices. It may involve significant costs in purchasing, deploying, managing, and maintaining those security devices, and device diversity is also costly [15][44]. Forrester [37] points out some key strategy to capture and measure the value of consumerization of IT, the following figure illustrate various costs with incurred on BYOD

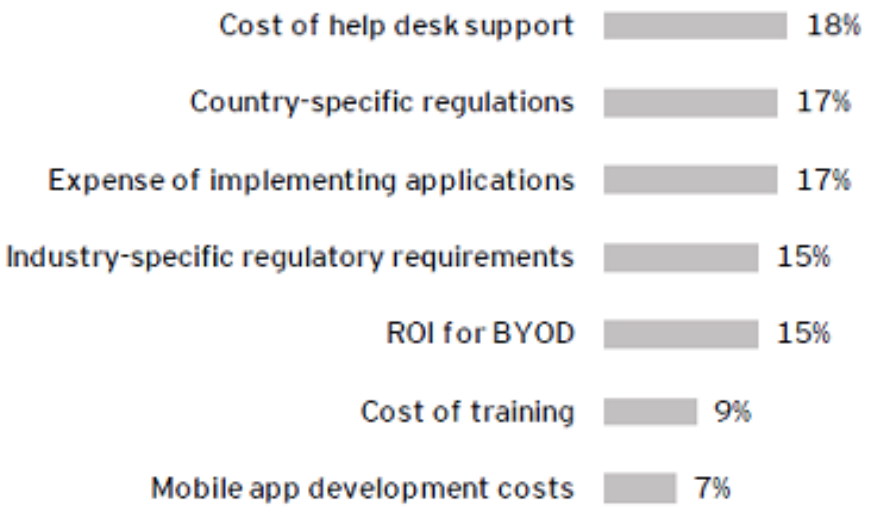


Figure 6 Hidden Cost of BYOD Implementation [37]

The figure shows the hidden cost of BYOD implementation. While there are, various costs incurred on BYOD, they are not seen as major barriers for deployment

The global security state of mobile devices, services, and networks are in critical condition. In fact, without suitable security solution the possible cost benefit brought by BYOD maybe lose, because of all the risks and issues we mentioned before which follows BYOD [1]. Therefore, it's crucial for organizations to deploy a proper security model and policy for mobile devices.

Ocano in his document [45] says, BYOD is saving money for the companies by not buying devices at all for users, and helping their employees to be more productive and innovative. But this value is possible if BYOD will implement in the strategic way. For benefiting BYOD's cost effect, there are two models:

- Basic BYOD model: it's typical implementing way of BYOD in companies today, which is incomplete patchwork of capability and policies, this can also be viewed as a median level of BYOD capabilities [42].
- Comprehensive BYOD model: this is more strategic approach and enables all BYOD journey and examine the benefit at each stage from no BYOD at all, Basic BYOD, and the comprehensive BYOD [42][46].

The major hard cost operation of BYOD coming from the following areas:

- Hardware costs: the employees will purchase the device, but previously bought by company.
- Support cost: Implementing comprehensive BYOD provides an opportunity support community like wikis, forums and other form of support. Cisco is one company that reduced support cost in this way [Cisco Interview].
- Telecommunication costs: It is assumed that enterprises lose some degree of purchasing power on telecom contracts because the users migrate from corporate data plans to self-funded plans and sometimes maybe user work perfectly with WiFi access rather than full cellular data access[42].

The latest Cisco's IBSG (International Business Solutions Group) Horizons analysis in the survey mentioned that, companies can gain an additional 1300 US dollar annually per mobile user with comprehensive BYOD [41].

Antonio Scarfo [39] says, the companies will embrace BYOD because this phenomenon instead of discouraging, it always the same in improving the companies productivity and reduce the cost.

Cisco's financial team IBSG valuing BYOD financial like the following model:

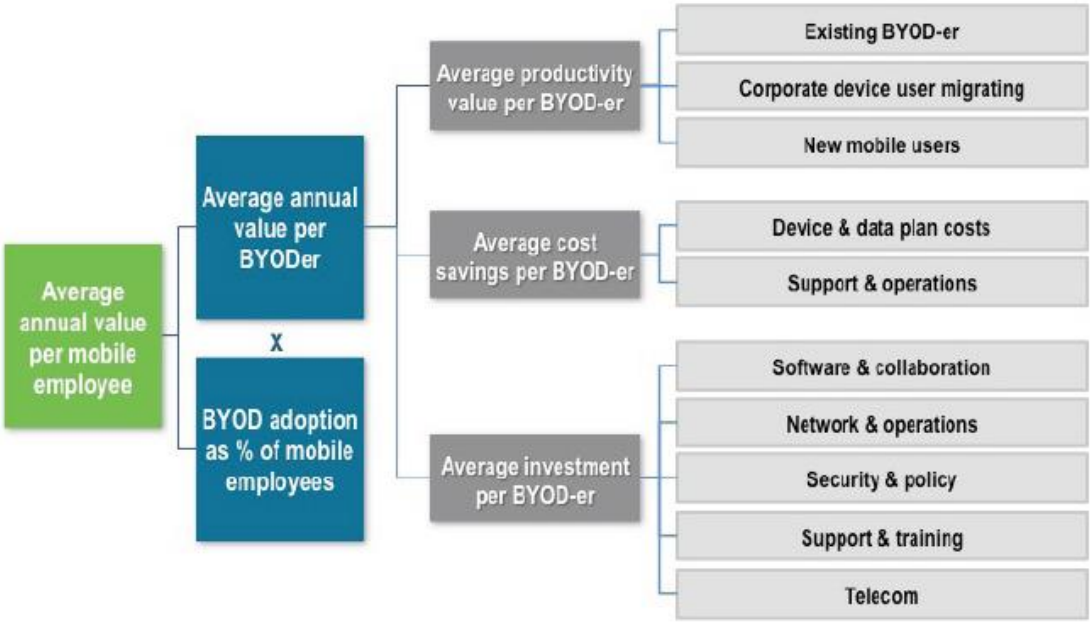


Figure7 Valuing BYOD: Comprehensive Financial Model [42]

The figure shows the elements concern to be costly in adopting BYOD to find an average of annual values per mobile employee

Cisco divide financial model of BYOD, they focus on BYOD-er productivity, the average cost saved per user is from device cost & data plan cost & the cost that will be save from support & operations, and the average of investment software & collaboration, network, security & policy, training, and the telecommunication as illustrated in Figure 7.

The research about cost analysis as mentioned above will bring us to think about two factors; one is saving cost and the other is the costs to adopt BYOD compare to the traditional companies owned device. The advantage of BYOD in cost saving as most of companies thinking about it, saving device costs, and the new devices

are prepared with a bunch of useful software which companies don't need to pay for the license, support & operation, device defection [UNDP Interview]. The users experience on their own devices will support companies to not worry about training them on the devices, beside the company will improve productivity, flexibility, and employees/customers' satisfaction as mentioned above. On the other hand, there are some disadvantages and hidden cost which makes companies spend more money than what they expected. Network management, applying security mechanisms, vulnerability management, data & data plan cost, software & platform for device management, the risk of device lost. In general, there are three main elements of costs (hardware cost, software cost, support cost), and those three main element costs can be used for saving or it may cost more than expected. Based on above mentioned and the research we can define the effective cost of BYOD like the following table.

Saving Cost elements	**Cost elements**
• Device purchases (part or full) • Device software • Device defection • Employees productivity • Employees satisfaction • Employees trainee • Customers satisfaction • Flexibility • Operation & Support	• Network management • Risk management • Data communication & data plan cost • Platform cost • Device recovery cost (lost, defect) • Security safeguard • IT management • Mobile device integration • Mobile app development costs

Table 1 Cost elements division

3.6 Summery

This chapter highlighted that this approach incorporates both individual and enterprise mobility that relies on remote access technology, as well as device mobility management and application mobility management solutions corporate with mobility of business process. Moreover, BYOD ensures the broad view of mobility such as, information, communications and access from anywhere, by anyone, from any device and at any time. BYOD is intensifying mobility usage to encourage organizations to use current technology trend and mobile usage, and enhances current growth. Furthermore, this study highlights the benefit of BYOD in integrating businesses and provides sustainable benefit with internal and external users, and reducing the costs by using proper policy and strategy. However, there are also risks associated to the use of mobile devices and there are challenges when devices access to the company's information through internet.

Chapter 4

4. State-of-the-Art

This chapter will explain the history of BYOD and its current state of technology to provide a deeper understanding and among other points and status will explain the BYOD architecture.

To understand the BYOD, in consideration with the literature review, it is necessary to gain basic comprehension of the technical issues at stake nowadays. On the market, there are several products designed to support BYOD, some of them are based on virtualization of the device, other offers specialized applications for specific business processes such as emails or VPNs and furthermore, some products offer remote connections to the enterprise networks, and some mechanisms to protect security purposes, such as access control, remote wiping devices.

Let's start by defining a few central concepts concerning the original design of mobile devices and security management and the status of the technology and security solutions.

4.1 MDM (Mobile Device Management)

MDM stands for mobile device management, Companies use this software to lock down, control, encrypt and enforce policies on mobile devices such as tablets and smart phones.

Figure 8 MDM

This figure shows the symbolic representation of MDM (mobile device management), which is a multifunctional framework that the companies use this to have a full control over the device.

With MDM software IT department of companies can have full control over the device. It is a multifunctional framework which gives businesses opportunity to control mobile devices [34].

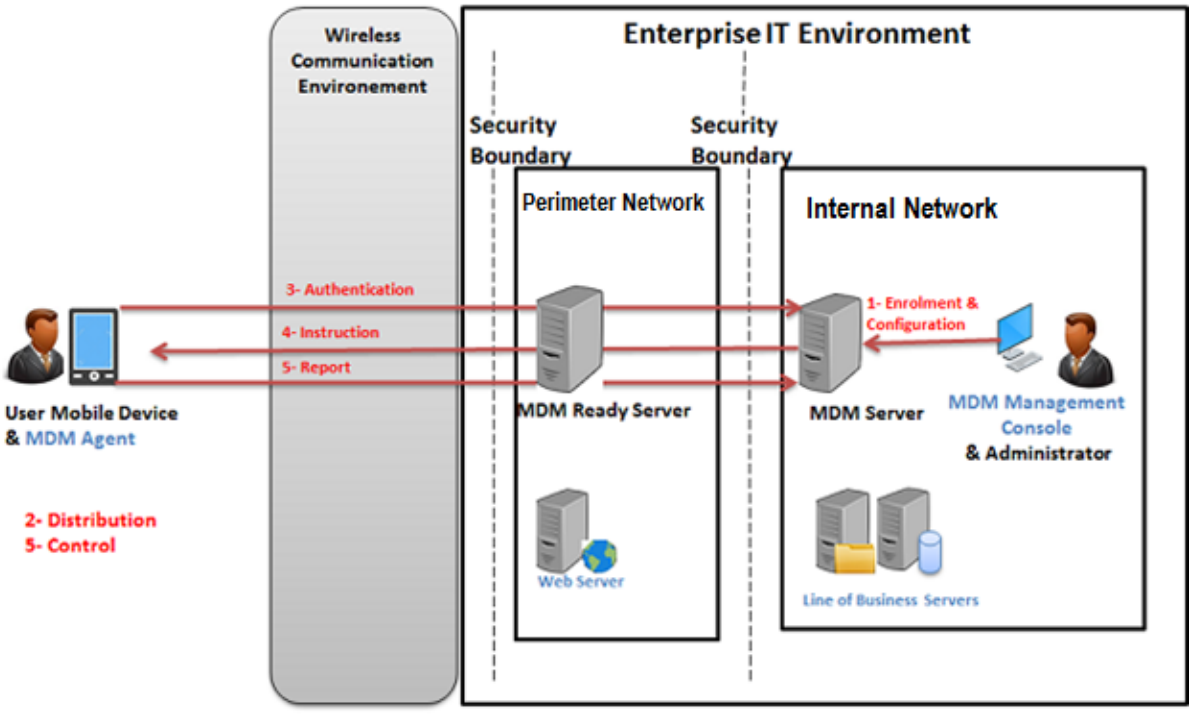


Figure 9 Mobile Device Management System [47]

This figure shows the steps to complete the operation of MDM (mobile device management) system, which contains of four components, can be done in 5 steps, but the step 4 and 5 are repeated regularly and as needed.

Step1. Enrollment/Configuration: In advance mobile devices configured and registered in MDM system like related to the Mobile device and user and the policy of each device.
Step2. Distribution: The MDM agent will be installed on the users' mobile devices. It can be distributed through application store or in-house.
Step3. Authentication: After the installation when an MDM agent runs, all the mobile device data (IMEI, IP/MAC address, phone number, etc.) are sent to the MDM server to verify whether they match the data registered in the system.
Step4. Instruction: If it is verified by MDM system then the MDM server sends back to the mobile device the control policy and commands like "remote wipe" according the mobile device status data and user.

Step5. Control/Report: The MDM agent will control the mobile device according to the related policy and command and send the results to the server [47].

MDM solutions contain a main component which manages protocols, provides constant control and monitoring. It resides within the company's network and relies on the exchange of certificates to authenticate and communicate with MDM agents which is installed on mobile devices. MDM is used by BYOD for companies and enterprises to implement a strategy that requires a centralized, simplified solution which allows businesses, companies and organizations to strictly control mobile devices [34]. MDM's main components are communicating with MDM agent on mobile devices to enforce access rights, update, synchronize files, trigger remote wiping, support VPN connections, conduct anti-malware scans, and provide activity reports[34]. This solution was awesome when the company owned the phones back in the days of Blackberry. MDM is a good solution for employee's owned devices if they agree to the terms and conditions related to this technology. But because now users use their own devices, they want to have their private applications and activities on their devices and do many personal things on them which is the main purpose of BYOD, MDM software is a bit heavy-handed and restricted for users.

4.2 Access Control and Authentication

To make sure that only authorized users can access to computing resources of the organization [15] and to ensure that the access is restricted properly, the organization should authenticate each connection before granting any access to the organizations' resources. Traditionally, enterprise set a boundary as internal network is trusted and external network is untrusted [36][48]. There are many ways to authenticate remote access users, such as with passwords, digital certificate, or hardware authentication tokens [36] these mechanisms will provide greater assurance for trusting devices to protect data and ensures access on the devices. If the password is the only mechanism of remote access for the authentication, then the authentication mechanism of organization should be different from the remote access authentication mechanism [15]. It can be assumed that sometimes some users will use the same password, but having different password will reduce the impact if one compromised the other will still stay secure that's why the password should be enforceable. The organizations with the need of higher security should not only rely on the one password, but they need a multi-factor authentication [15].

4.2.1 Multi-factor Authentication

Multi-factor authentication is using more than one factor for the authentication; it is combining two or more independent credentials This method is to make it more difficult for unauthorized people to get an access to the target. This is because if the attacker managed to break one factor there is still at least one barrier more before successfully reaching the target [48]. Multi-factor authentication is typically recommended for confidential data, such as username/password combination and additional factor such as answering challenging questions or biometric identification [49]. But this technic will be an interesting challenge in particular for mobile devices, one challenge is, many strong authentication technologies are not compatible with many mobile devices for example (smart card, USB token), another one is, there are number of two-factor authentication technologies have been used by mobile device [10], so what will happen if the mobile device is used as an endpoint and it is the authenticator.

4.3 Remote Wiping Device

Remote Wiping is a mechanism that an organization used when they want to remove/delete the data and applications stored on the employee's device with respect of the reasons of employees/owner of device when they want to separate from the company or the device disappeared for any reason lost/stolen, most of technologies solution for BYOD are providing this solution such as MDM, MAM [10][Henrik Staer, Cisco Interview][Ognjen Krstulovic, UNDP Interview]. But different kind of technologies have different capabilities in using this mechanism, for example, MDM technology is capable to wipe the entire data and applications and document on the device, but MAM is capable only to delete all the data related to the company and leave the personal/private data and applications remain on the device[34][50]. Mark Bermingham, security vendor, says using reactive security approach as remote wiping data from device is a shortcoming of MDM, because it happens after a problematic event occurs [50], because in some cases hacker can turn off network access from compromised device and making it impossible for company to transmit the erase-data command. And MDM doesn't prevent hackers attack to the employee's mobile devices or a thief from stealing the device and accessing sensitive data, that's why companies need to have proactive measures like date encryption and antimalware software[50].Ognjen Krstulovic, UNDP interview also mentioned other problem of remote wiping; an incident when one of their employee reported lose her device, the IT admin immediately changed the password but afterwards, they were not able to execute remote wiping command.

4.4 MAM (Mobile Application Management)

MAM stands for Mobile Application Management, which is alternative of MDM but it concerns to limiting mobile users' access to applications, and protecting permitted programs and data they use on the mobile device[50]. MAM allows the company to apply security policies, lock down, define access control rules, configure software behaviors, remote wipe applications under its control, restrict access to unauthorized applications and install approved applications [34]. One of the method for applications security of MAM to manage data leakage to unauthorized people is blacklisting policy within mobile

application system that allows device to be selectively wiped, or blocked when the system detect a blacklisted app [51].

Figure 10 International Airline Uses Apperian Alongside AirWatch[52]

This figure shows the corporate liable devices for managing devices and applications used by airline by using MAM and MDM.

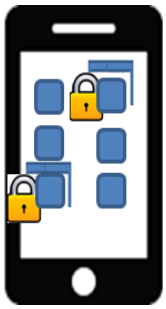


Figure 11 MAM

This figure shows the symbolic representation of the MAM (mobile application management), which is the alternative of MDM and is based on software solution (Author)

The above figure 10 is Enterprise Mobile Management based on two approaches; one is corporate liable devices or devices the company owned which uses AirWatch solution for managing devices and applications. But for its fleet of BYOD users they use Apperian solution to distribute secure policy managed applications to device that are not registered and enrolled in a MDM profile. Both communities are run independently but have a consistent security stance, giving the company flexibility to support a diverse device ownership environment [52]. In the above example on why MDM needs to use standalone MAM is because MDM alone is insufficient for deploying mobile apps securely to the potential users.

MAM system is used by IT administrators to remotely install, update, audit, and monitor enterprise applications on mobile devices [1]. Applications standing out of MAM's boundary remain private under users own control. MAM is more proactive when combined with containerization. For remote wiping, the company could just wipe the corporate apps and data, but user's personal apps and data remain and most importantly when using MAM, the company doesn't have any visibility to the user activity on the device outside of their apps[51][1].

One of the key trends in the market that may influence the demand for stand-alone MAM is the emergence of cloud access security brokers, CASBs, which enable access and authorization control over cloud-based resources like cloud-based CRM for mobile devices. This tool acts as an intermediary between a device and the service like SaaS application or email server. They are making their way into the mix of enterprise toolkits for managing mobility and their growth and evolution could certainly stem the demand for MAM tools in the future, depending on the specific needs of the organization (Gartner).

"MAM platform can deploy the app safely to any user's device and effectively enables the organization to distribute the app to any user throughout the extended enterprise including those users where MDM-based approaches are not possible or desired, such as BYOD, contract workers, dealers, franchisees, and those who's devices are managed by another organization"[53].

4.1 MIM (Mobile Information Management)

MIM stands for Mobile Information Management which can be describe as cloud-based services that sync files and documents across different devices and simultaneously administering security procedures such as malware scanning, for example Dropbox, Microsoft SkyDrive, Google Drive, etc.[34]. Data located on the service provider's server such as cloud server and the client can connect or access per the permissions of the device and the application. This product can be used for larger service offering which IT provides to the users like emails and calendar. But MIM cannot deliver the client apps to the devices therefore, MIM works with MDM or MAM to deliver the applications to mobile device's BYOD models such as MDM, MAM, and MIM provide basic solutions for how

mobile devices can be used or how data can be accessed in four major categories such as:

- Identification and access control
- Data protection
- Application security and Integrity
- Compliance”[1]

The above technics nowadays, for managing mobile devices, applications and information are not enough because the mobile devices networks are being targeted, that’s why there are more technics to take control of mobile device security.

4.5 Mobile Virtualization Models

Virtualization is creating a virtual copy rather than actual ones including OS, Desktop, hardware platforms, storage devices, computer network devices, etc. to deliver to any endpoint from a desktop or laptop to a smartphone or tablet. Desktop and application virtualizations are growing trends, it comes from the need of reduce cost and improve security and IT services availability [39], and the most common reason of using desktop virtualization is to allow users to run application for different OSs on a single host [54]. With mobile desktop virtualization, users are running secure applications and operating systems by connecting to secure in-house computers such as servers which are set up for this purpose, or they can be the users’ own desktops [55][39].

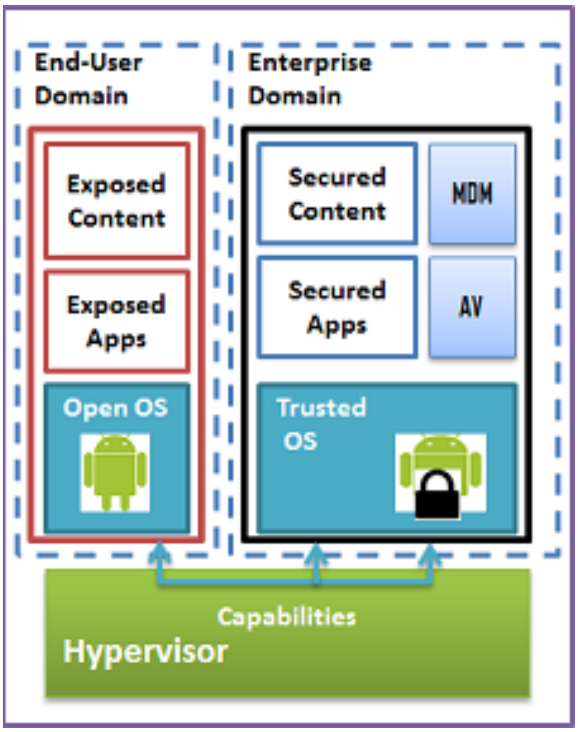


Figure 12Hypervisors on Android Phones from Verizon [Google]

This figure depicts the mobile virtualization model, a hypervisor on an Android phone. Mobile virtualization is a kind of containerization, which each user participates in mobile device, which will have a virtual portion on the container for holding corporate data.

Mobile virtualization is a kind of dual-persona technology or containerization, which each user's mobile device which participates will have a virtual portion on his/her container for holding corporate data. In some cases, there are two virtualized containers, one for work data and one for personal. Mobile virtualization makes device management easier because IT only needs to manage the virtualized portion of a user's device [55].

Remote access services are supporting mobile desktop virtualization to access and deploy remote desktop services and applications.

The biggest advantage of desktop virtualization is that the organizations' sensitive data will remain in the secure environment inside the organization, it will never be stored on the device itself, the file will transfer only when remote-access service supports transformation and the transformation permitted in advanced.

4.6 EMM (Enterprise Mobile Management)

The aim of managing an enterprise is implementing the right technology to ensure that employees are enabled to be productive while they are on the go. Ensuring a mobile productivity is one of the top priority and pressures companies to adopt mobile technology. Having right applications up- to- date on the right device is necessary to maximize employees' productivity and minimize wasted time [56][23].

Enterprise mobile capabilities are improving and go a long way with workers who have experience on mobile devices, but this is not enough because on top of the infrastructure it is required to support a mobility initiative. It is important that organizations have the right training for workers to empower workforce to take the advantage of mobility [56].

Thus, having the right knowledge and right technology in place, the companies can see benefits and productivity of mobility. This mobility in enterprise will bring some security issues to the company that's why the enterprise or companies will use a suitable technology and security technics to ensure security of mobile connectivity and employee's productivity by mobility[23].

The following figure is an example of enterprise mobility management to ensure the security and connectivity to users accessing data and identifying an authenticated user.

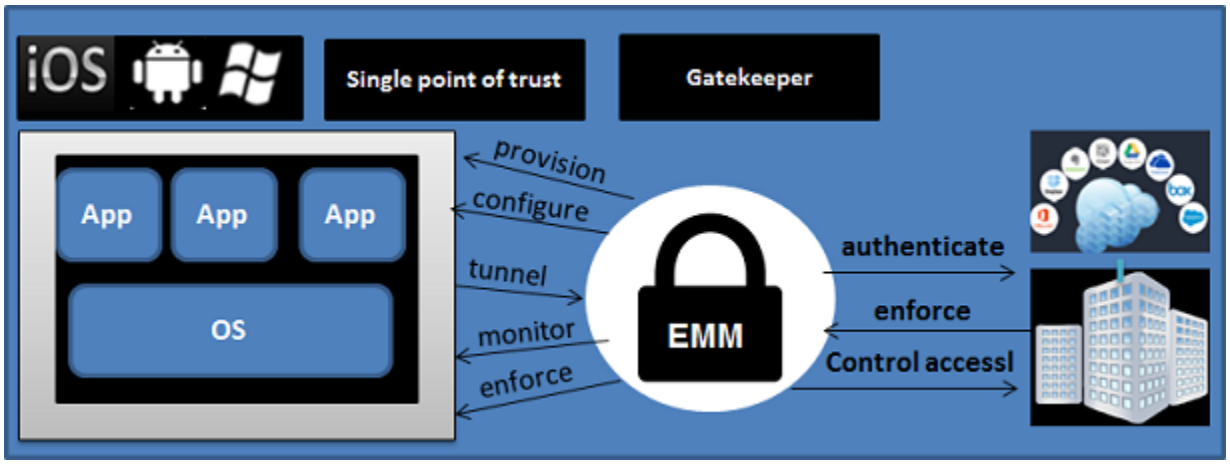


Figure 13 EMM One Security Parameter [57]

This figure depicts the EMM (enterprise mobile management) security parameters

The modern EMM platform can get a lot from modern mobile devices and MDM technology as mentioned above: but many are also asking for standalone mobile applications without MDM. But EFSS (Enterprise File Sync and Share) is now replaced by other mobile technologies widely accepted and spreading rapidly[58].

Mobile devices come with email and browsing on their own, but EFSS can securely share files such as documents, photos and videos across multiple devices and with multiple people (Figure 13). The synchronization, or copying, capability allows files to be stored in an approved data repository, then accessed remotely by employees from PCs, tablets or smartphones that support the EFSS product.

Many EMM platforms can now be integrated with identity and security products, for example, identity providers can make access decisions based on device status and security products can use EMM to enforce policies or remediate threats they discovered[58].

4.7 Dual Persona Devices

Organizations need to separate corporate and personal data to accommodate BYOD users while avoiding compromising data security and management [55] [59].Dual persona refers to the provisioning of two separate environments on one mobile device. It is creating two separate spaces or two profiles, one of them is managed by IT control and the other is managed by users. These two separate spaces will help to improve the security of enterprise data and it can survive users from losing all their apps, private data such as songs and vacation pictures etc., if an admin should perform a remote wipe. But dual-persona technology is still new, so a lot of information is up in the air[50]. The dual space can be achieved by software or hardware-based approaches; the first approach is software-based which involves the use of hypervisor or virtual machine monitor to run two different profiles and each with its own operating system which benefits the full capacity of the hardware and resources [60].

The second approach is for all corporate data and applications to get containerized on the device which is often done by MAM. This concept has become popular as companies

realize that it's valuable to separate private data from corporate data on employee's personal devices [50] creating an isolated area to centralize the containers in it and the specified profile can be used to access the enterprise data, and launch enterprise applications, and be subject for IT control, deploy IT policies, password protection, encryption, and remote wiping in the case of loss device or stolen or workers leaving the company. The users can shift between the two profiles easily without one affecting the other [60] [59].

4.8 NAC (Network Access Control)

Security technologies and products has created a new IT environment; NAC technology verifies security stability, it inspect the user of devices if they are compiled to the security policies before they access to the internal network [10]. NAC solution is blocking network access when an infected device tries to connect to the Enterprise's network to keep un-authorized device from internal network. NAC identifies and controls authenticated users or devices and enforces access control policies and compliance with the security policies of switches and routers [10][24]. This technology is commonly used in enterprise's internal network. Once a user is registered to the system, they will be identified to the network by providing the identifications before any activities happened, even for connection, they should be complied to be approved to use the network. Sometimes, devices will do the configuration, the device should be registered to the system and the un-identified devices by the system cannot be served. In having a secure BYOD environment, it needs to develop dynamic access control technology based on context information. This technology in the real-time will detect abnormal access and use of terminal devices on the real-time basis; it will gather information about the devices under agentless mode. This system contains a collection system, a detection system and a control system. It is collecting information by following user's authentication when the user's terminal devices connect to the corporate network, the detection system will analyze this information then the abnormal malicious behavior will be detected. The detection result will send to the access control in the system and according to the result the access will be controlled by the method like dynamic change of access privilege by legacy security equipment, and this process will be monitored and controlled until the use of network has ended [24].

In the collection system, the information that is collected is basically agentless the users and devices information are collected as much as possible by using different methods including DHCP fingerprint. The agent will install for the users/devices in the case of detection of abnormal behavior or malicious activity the agent will install to retry to access to the network because it's necessary to collect the information's accuracy this time, this policy will minimize agent installation.

In the detection, system users' normal behaviors are determined in the database system, profiling of each user is necessary, in this system profiling is a set of data objects, each object identifies a specific behavior, when abnormal behavior has access and use of corporate network detected it will compare with normal behavior record in the system, the elements will be the real-time context information of each user like access time, location, previous record of user's behavior and so on.

And lastly, the control system will react according to the detection result and policies and the access control through legacy such as firewall, NAC, or MDM [24].

4.9 Chapter Summery

This chapter presented the different technologies that exist and are available in the market regarding to the (State-of-the-Art), followed by little description of each technology and the purpose of those different technologies. Those technologies are used for different purposes in BYOD phenomenon. The chapter ends with an overview of BYOD's security and security architectures diagram.

Since BYOD phenomenon started, it has adopted and implemented many strategies, solutions and policies. There is no existing BYOD solution that satisfies all the conditions of management and security, that's why it depends on the purpose of used from the organizations [5]. Despite the benefits for both employees and the businesses, in fact, the employees became more flexible and comfortable at work by using their own device and applications, the organizations gaining employee's productivity and collaboration, the organizations are still doubting to embrace this phenomenon because of some unfortunate security issues arising from different devices accessing the network [61].

Chapter 5

5. Theory and Considerations

Theory is one of the most important part of the research report. The theoretical framework is a structure that can hold or support a theory of a research study. In this paper, I am going to focus on 11 functional areas of enterprise cyber security as a framework to do my research in analyzing the security issues and security risk managements associated with BYOD on organizations and enterprises.

5.1 The 11 Functional Areas of Enterprise Cybersecurity

To provide the employees needs and offer mobile access to corporate system, and increase the productivity, better users' experience, competitive advantage of the companies, and deduction of the cost, these disruptive mobile technologies are forcing organizations and enterprise to adopt their business strategies based on BYOD strategy and policies. With these increasing flexibilities and advantages, the security is very fast becoming a top priority. Organizations need to plan for the protection of these devices and integrate with their overall endpoint, server, and security functional area strategy [10][Cisco Interview].

ISO 27001 focus on five principles for security requirement which are crucial for enterprises that implement BYOD policies, the five principles are; Confidentiality, integrity, availability, access control, and non-reputation [23].

What has been mentioned and researched until now needs to revise the 11 functional areas of enterprise security, and we will consider how each functional area should be adopted to provide enterprise protection on BYOD's end.

This approach is directly tied to the risk assessment process and uses to organize an enterprise cybersecurity program. This assessment measures each functional area's effectiveness to determine which functional area is the strongest and which is the weakest. The 11 functional areas in enterprise cybersecurity have almost equal levels of

capability and impotency, which means, if one functional area is weak than the other functional areas should be prioritized for improvement. Thus dramatically simplifying the enterprise cybersecurity strategy, prioritization challenge and mitigating risks [10].

Figure 14 The Eleven Functional Areas of Enterprise Cybersecurity [10]

The figure depicts the eleven functional areas of enterprise cybersecurity, which areas directly tied to the risk assessment process and are used to organize the enterprise cybersecurity program.

1. **System Administration:**

System administration is for securing the administration of enterprise and security infrastructure, to protect the administration channels of the system from compromise. System administration protects its own functional area because if an attacker compromises this area it will easily disable the whole system and bypass the rest of enterprise security system [10]. System administrators and computer security program managers are responsible for technical aspect of preparing, operating, and securing remote access solutions and client devices[15].

The analysts of Cybersecurity observe that system administration channels become very popular target for deliberate attackers for some reasons; one reason is because nowadays, system administrators have control over hundreds and even thousands of

enterprise computers often from a single console. Another reason is, system administration's security relies on insecure protocols and username/password authentication. Finally, it is because System administration's technology is relatively immature, with few built-in checks and balances to detect malicious activity or prevent it in the first place [10].

System administration is the powerful function area in BYOD's architecture, because it is the Administrator who defines the user's policy to protect the confidential data in the system from unauthorized people. All the rest of focus areas are related to the security administration having to deal with them to solve the problems and require their attention. For example, in the MAM system solution, IT administrator can remotely install, update, remove, audit, and monitor enterprise related applications on the mobile devices [1]. Basic rule for system administrators is that they should not perform duty actions from mobile devices, and they should use full endpoint protection capabilities to protect and monitor their assets [10]. The system administrators can use the capabilities of isolating network and protocols and can provide cryptography protection for the system administrator, and as mentioned above auditing the system to detect malicious activity and detect attacks. Administrators can manage BYOD devices remotely, they can also set customize authentication checkpoint on apps or data or restrictions to device features and settings[40]. The potential benefit of system administration is that it allows systems administrators who are on the go, who needs to perform their duties at any location any time without them having to overshadow the security risks [10].

2. **Network Security:**

Enterprise uses network securities to protect its network from unauthorized access. Network security detects intrusions against the network and the computers connected to it. In addition, the network architecture and its defenses can be a channel to connect user and attackers to do their activity. Because mobile devices primarily use external networks to access organizational network, and use Internet to access, organizations don't have control over external network which the devices use [14]. Network security needs to be considered for preventive controls such us firewall to block attackers activity, detective control such as intrusion detection to detect attackers' activity which cannot be blocked,

monitoring controls that capture activity as input to correlation engines that support forensics and investigations [10]. Detecting and documenting anomalies within the mobile device infrastructure through monitoring, such anomalies might indicate malicious activity [10][14]

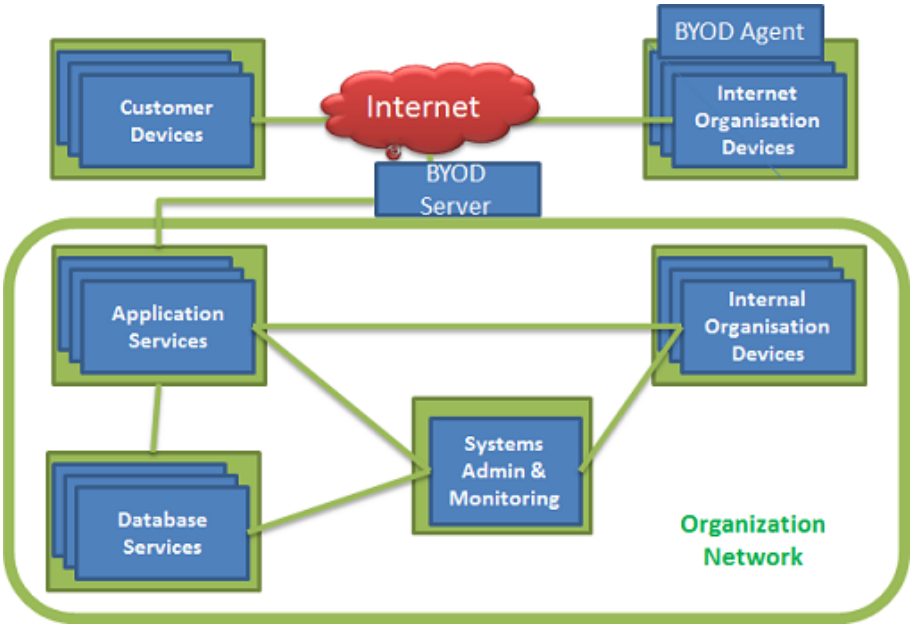


Figure 15Simply Stated, Enterprise IT Security Involves Hardening the Enterprise IT Components [10]

The figure illustrates organizations network and external device connection through Internet.

Network security's goal is to protect the enterprise's network from use or attack by an adversary and the objectives are; to prevent and block malicious traffic from passing in from one part of network to another, to detect malicious traffic while it's in transit, analyzing network traffic in order to identify malicious activity or to generate artifacts indicating the lack of malicious activity [10]. Organizations should consider using separate network for all external client devices, including BYOD and third-party controlled device instead of permitting them to connect to the internal network directly [15].

The most dynamic aspect of network is for data flow to remain secure, the network capabilities providing visibility and providing the protection against internal and external mobile devices threats. Network security can block unauthorized devices, unauthorized users and non-compliant apps [7].

ISO organization in ISO7498-4 identifies five functional areas which need to be satisfied in order to maintain control in networks on OSI management model[21]:

- Fault Management
- Accounting Management
- Configuration Management
- Performance Management
- Security Management

Intrusion detection and intrusion prevention systems are classified as monitoring tools which can be beneficial in network security for BYOD[21], firewall antivirus, routers and switches are capable to implement security mechanisms. Wireless networking can be used for network security to protect network from unauthorized access; SSL and TLS encryption can be implemented for secure communication. The best defense in response to litigation arising from a data breach is to demonstrate that the company actively attempted to mitigate threats inherent in its business model[26]. Creating a VPN in BYOD devices will secure enterprises network environment for the traffic when it comes from Internet, so the enterprise can look for evidence of unusual connections [10][36]. But encrypted remote access cannot be examined by firewalls and intrusion detection system or other network security mechanism, that's why remote access architecture should be designed so that the communication can be examined by the appropriated network [15]. Digital certificates and two-factor authentication provides a more secure method to access the network[6].

3. Application Security*:*

Application security involves security measures that are specific to certain applications or protocols running over the network. The applications that most in need of security are those that communicate over the network and are accessible from the internet; E-mail security, Application-aware firewall features, database gateways and forward web proxies [10][15].

Figure 16 Application Development Securities (Author)

The figure shows the application development securities that involves security measures to certain applications or protocols running over the different network

Application security's goal is to protect the enterprise's applications from use or attack by an adversary. The objectives of application security are; prevention, blocking of malicious operation against applications and communication protocols; detecting attempts, to exploit and compromise applications for malicious purposes. Forensics is collecting log data about applications activity that can be used for audits and investigations of incident; and the auditors collecting evidence and items from the log data as well, so they can suggest that applications are safe and not being used or manipulated by attackers. Security of applications are important because the application software indicates the flow of communication between the application client and server software [10][15].

The number of application security being developed by each organization is increasing year after years as the number of mobile apps is rapidly growing; each app becomes a potential channel for malicious or involuntary software and an inconvenience to distribute sensitive data or intellectual property. That's why enterprise should have a protection for any mobile app, data connection, and access [49]. There are security technologies for most part of applications to protect consumer's data when an enterprise adopts BYOD

[10][36], some of the technics and capabilities can even use for applications which are even normal in the public facing like e-mail for example. There are several technologies to protect BYOD applications, but the system cannot protect every single application, because as mentioned before, app development is growing rapidly and the vulnerability comes with this growth. Mobile Application Management, applications container, Dual Persona etc. are the technology developed to protect applications used by BYOD system and separate business related applications from private applications on the same device (more details in the chapter 4 state-of-the-art).

4. Endpoint, Server, and Device Security:

Endpoint security is determining how remote access servers and client devices should be secure, it is a protection and detection of endpoint computing devices such as, Personal computer, servers, and mobile devices [15]. No matter how hard an enterprise tries in defenses and protection the number of compromised endpoints will never be zero, that's why an enterprise should apply the rest of security functional area to compensate this security shortcoming and minimize risks as low as possible [10]. Many enterprise's endpoints are outside of its control and belong to the partners, customers, and users or third-party that's why enterprise have to consider the security of these devices as overall risk analysis and consider on how to compensate for their possible vulnerabilities by other protections[10][14].

The goal of endpoint, server, and device service security are; to prevent attackers from compromising devices or taking control of the administration of computing device, to detect the attempts that maliciously use the device; and to facilitate investigation of incidents when compromise is suspected. Endpoint security is a big opportunity to make it difficult for attackers to enter to the system: it can set alarm to detect attackers and improve detection and response when attacks occur [10][14].

These functions are most weakened in BYOD because enterprise or companies do not control all users using their mobile devices. Without MDM technology it would be hard to provide outstanding protection for enterprises adapting BYOD [10]. Deploying digital certificates to endpoint devices are required to provide security and flexibility and enforce

different security policies, regardless of where the connection established. This solution focuses on providing digital certificate enrollment and provisioning while enforcing different permission levels [6]. The objective of endpoint security is to prevent attackers from taking control of the devices, to detect the attempts and identify maliciously used device, and to facilitate investigation of incidents when compromise is suspected. MDM is one of the top capabilities of device security and endpoint in BYOD it's the same as PC computer and company owned device, we need to implement the security defense and protections, endpoint encryption, access control, VPN, application white listing, malware detection, and user's privileges to secure end devices in BYOD.

5. Identity, Authentication, and Access Management*:*

Identity, authentication, and access management supports all other security functional areas by providing answers to the following questions:

- Who is accessing enterprise IT systems?
- How are they identified?
- What can they access once they are authenticated?

When an enterprise is in an isolated system without access from outside, the physical connection is a matter to access the data, in this way its expected connection should be authorized and identified in one way or another. But when the system is connected to the Internet it would have problems, because too many people online are only a click and password away from accessing system and organizations data. Identity management ensures the provisioned and de-provisioned access account and periodically re-certified per enterprise policies. Authentication makes sure that appropriate technologies are used to identify users who are accessing the enterprise system, and the access management ensures that the privileges on enterprise system are provisioned and de-provisioned[10]. NIST guidelines [15] say, that the organization can determine whether the device should be permitted to use the remote access and what level of access will be granted, it can limit the access to the internal network, deny access to the network, or access with requirements. And NIST contentious [15], the identity, Authentication, and access management is to ensure that authorized people can access to the resources in the

system of enterprise, to ensure that the access is restricted properly. The use of authorization technologies is to ensure that only the necessary resource can be used. The goal of access management is straightforward, that means the access is either allowed or denied, and the same for the authentications and identity, except for the fact that the permission and privileges are changed for the users by system administrator [10][15].

From the technology standpoint, it is how people will be able to access enterprise applications to provide secure access to data and applications in terms of people, and how to incorporate their data and files on their personal devices[7] this functional area is a compensation for BYOD security challenges [10]. Enterprise has to continue to provide and develop the environment that offers the customize access and experience based on identity, while BYOD creates seamless integration of app environments across platforms [37]. Strong authentication, especially to protect an account from being compromised on the endpoint mobile devices, Multifactor authentication is one of the best options [10]. However, it's important to remember even strong authentication cannot protect from seasoned hijacking attacks. Another effective protection is controlling accesses to minimize the potential consequences of compromised endpoints and compromised credentials. In the basic scenario of BYOD, we should answer three main questions in relation to identity and access management, who is accessing? How to identify? And finally, what they can access when they are authenticated? Cisco in the building architecture document [6] wrote, the capability of BYOD to this functional area is to use SSL, TLS, digital certificate, key protection, one time password, and data encryption to secure this area in BYOD. BYOD's solution for identity and access management uses different technologies to manage them, such technology for example when MDM agent in the case of MDM needs to install the device to be identified and authenticated by the server system and have an identity key and the SSL technic used to this key exchange.

6. Data Protection and Cryptography:

Data protection and cryptography is one of the most important functional areas of security to protect confidentiality and integrity of information owner [15]. Cryptography has only been used to protect military communication and almost all its Internet communication and commerce. The client must trust that it is communicating to a legitimate server side and vice versa, the data should only be reached by a credential and authenticated people. When the data is transferred through, the network should not be changed and read by unauthorized people. Cryptography protects data at rest and in transit, and provides for strong authentication and non-repudiation for messages and data, supporting message identity and authenticity[10]. Protecting corporate business related data such as, emails, contact list, calendar, and corporate data like sensitive information passing over the Internet, wireless network and another untrusted network from remote access communication to have its confidentiality and integrity should preserved by use cryptography [15][33].

Data protection and cryptography's goal is to protect the confidentiality and integrity of data by using cryptography technique, digital signatures, and key management. The success of the technique depends on key management. In addition to cryptography, it means protection of storage data, providing confidentiality and integrity by restricting access confirmation to authorized system entities (users, process, devices) through physical and logical mechanism, because many mobile forensic tools are available to retrieve and collect data from mobile devices when it is lost or stolen [33]. For protection, confidentiality and integrity of data, each enterprise uses cryptography technics as encryption and digital signature. Data protection and cryptography have four major objectives [10][15].

1) Prevention is to protecting the confidentiality and integrity of enterprise data by using cryptographic technologies.

2) Detection, enterprise-monitoring cryptographies to detect a weak cryptography or breaches when it is occurred.

3) Forensic objective is to track the cryptography used by enterprise.

4) Auditing objective is to collect information about keys strength of used cryptography and ensure that comply enterprise requirements for protection[10]

The companies and enterprise needs to make sure that their data are encrypted per company's policies and ensure where and when the employees have been using it (Gartner). Enterprise should make sure that corporate data is secured and protected, there is no one size fits all solution. Any BYOD policy requires a platform for maintaining security, because it may carry sensitive corporate data and those data should not be stored in the plain text on the devices [33]. Mobile Application Management platform is an effective and well thought out system to help enterprise to ensure that corporate data is secure, and MAM platform support IT personal to enforce policy to the BYOD devices and the action like remotely wiping corporate data on devices in the case of lost or employees leaving the company (more details under section 3.2)The data should be protected at rest and in transit to protect confidentiality and integrity of data on the devices and to the network; this functional area has not been benefited with regards to personal devices. That's why in the future mobile devices will store credit cards, payment information's and more sensitive data and those data should be secured over the Internet, the attackers are not able to compromise and use those data even if they take control over the device if the data is encrypted [10]. The capability is general awareness of need for security measures, such as encrypting information or using SSL[62], using trusted platform model, cryptography tokens, one time password are possible to use [10].

7. Monitoring, Vulnerability, and Patch Management:

Monitor the status of the enterprise's security and maintain that security over time by identifying and patching the vulnerabilities as they become known and update software at the right time, define and implement the patches software developer providing when they define vulnerability [63]. Mobile device risks and threats are on the rise, more specific vulnerabilities, malware, and network attacks. What can be seen is an increase in mobile device compromises, device vulnerabilities, and malicious apps [51]. Compliance checks provide information about whether a device has remained compliant with a mandated set of policies and detecting anomalous behavior by observing the activities of mobile users measuring activities and compare this measure with baseline of known normal activity

[36]. Patch management is, as soon as a vulnerability observed it should be resolved and stressed the importance of maintaining an up-to-date that has resolved past vulnerabilities on the mobile devices [51].

The goal of monitoring, vulnerability, and patch management is to understand how security changes over time. When the system is quiet, it means everything is well, but the problem is if the attacker identifies the vulnerability of the system and attacks while the system is vulnerable. This functional area involves maintaining security over time; the risks may constantly be re-assessed. The major objectives are; 1) prevention which ensures that vulnerabilities are compensated and patched before exploited by attackers. 2) Detection involves to monitoring all enterprise security automation system to detect incidents so the incident will be investigated and remediated. 3) The forensic objective is when the incident is crosschecked and investigated. 4) The audit objective involves centrally collecting forensic data that can be analyzed by auditors and investigators [10].

Monitoring, vulnerability, and patch management's capabilities focus on maintaining enterprise security if it's ongoing correctly and detecting incidents against enterprise security systems. Monitoring provides analysis of logging data from the infrastructure and processing it to identify interesting event, vulnerability capabilities scan infrastructures and computers to identify vulnerability and remediated [10][36].On one hand Enterprises are legally obliged to inform employees about monitoring activities [23], on the other hand, they are not able to monitor mobile devices endpoint or BYOD endpoints while they don't own the devices. Endpoints are available to be compromised no matter how hardened operating systems are protected, regardless they are protected by enterprise networks or taken home and connected to the Internet [10]. Meanwhile, enterprise can monitors its own system like, if there's several times of login fail, or detect unusual connection pattern, or a set of credential used in different countries [10]. Reacting to the vulnerabilities immediately to prevent from compromising and patched, especially for untrustworthy developed applications (More details about vulnerability and patch management on section 3.3.3). Monitoring is important to detect the vulnerabilities and prevent the system from this incident and patch management is to remedy the vulnerabilities to protect the system from incidents. The capabilities of this functional area is in performing system

monitoring as mentioned above, data analytics, system network monitoring, system change detection, and patch management deployment for untrusted applications. Motorola uses DRM protection to keep control over personal content and the device integrity can be ensured by using TPM installed on the device to monitor the integrity and enforce the received policy[10][64][65].

8. High Availability, Disaster Recovery, and Physical Protection:

We cannot talk about security without physical protection. Cybersecurity functional area put physical protection, disaster recovery and high availability together as a logical group because, they defend the greatest threats to protect availability, physical security control which is a major security concern in BYOD [15][10].

Availability of physical access to malicious will make it easier to achieve breaches of confidentiality or integrity, internal resource accessed by remote access should be protected against expected threats, especially mobile devices are small sizes and easy to transfer and the capability of lose and being stolen is higher than server machine and PC's [15]. Physical access makes long-term way of breaches shorter to malicious; an Enterprise can balance disaster recovery with levels of physical protection to achieve cost-effective, business continuity, and capabilities.

High availability, disaster recovery, and physical protection are operations and maintenance; it is security related task for business continuity and requirement satisfaction, which may cause a routine technical failure, natural disaster, or man-made catastrophes, the system should be protected and can be quickly recovered[15][10]. In this functional area, instead of talking about prevention and detection the enterprise is concern about reaction capabilities. The overall objective is to ensure the ability to respond the disastrous situations, perhaps the most important is how enterprises create mobile data backup, and how to recover the data during disaster recovery, or reaction capability in the case of cyber-attack, mobile device lost with enterprise confidential data, and natural disaster[1][10].

This functional area is capable to make IT system robust, having the same data in multiple locations and protecting physical devices that stores enterprise data or delete data from

the devices when it's lost, because this functional deals with availability, it considers to the data confidentiality and integrity, because sometimes when the enterprise security makes it difficult for attacker, then the attacker will target physical attack[1][10].

Physical protection for BYOD is a big challenge because as we mentioned before, mobile device protection is so important as mobile devices are small in size and they are mobile, which is why they are very possible to lose or to be stolen and it will be easy to sell it in the black market [64]. Data ownership and recovery should be the main point in the policy settings. Personal device and corporate device should have different security policy and application distributions; the shift from corporate laptop to mobile devices has consequences for data recovery when a device is damaged or lost [37], or due to small dimensions it's possible for smartphones to be stolen or lost more often than laptop, during this period the device is not available for legal owner, it's possible for the malicious to install spyware on the phone, so afterwards it can read personal data, contact lists or messages [64]. The physical protection in BYOD should be a concern and it's always good to be aware of losing the device, and the device data should always be updated; if in any case the devise is lost or damaged, it will be immediately reported to the IT department or sometimes the user can use another device to login to the system remotely and activate wipe the data on the device (Cisco Interview, UNDP Interview). This functional area is important to fulfill and follow to business continuity, and in a matter of accidentally wiping data on the device or device defection; these unfortunate instances should be able to recover in the matter of business continuity.

9. Incident Response:

This functional area is about responding when the incident happened, no matter how strong the defense system is, the incident will occur, and the risk will never be zero. Incident response has become an important component of information technology, the organizations should consider incident involvement and how it should be handled and plans should be documented as well [66].

Incident response does not protect enterprise and mobile devices from attack, but it will respond when the incident has occurred. The incident response process is a multi-step

process that consists of investigating, reporting, containing, and ultimately remediating the incident [10]. It is critical to respond quickly and effectively when attacker compromise a personal and business data or the security breaches occur. Incident response became widely accepted and implemented because of the capability of systematically response to incidents [66].

The incident response helps to minimize loss or theft of information and disruption of service caused by unfortunate incident. Incident response includes; operational disruptions, security incidents, deliberate attacks, natural/man-made disasters, mistakes and accidents. Incident response's overall objective is to understand what enterprise vulnerabilities deliberate attackers will attempt to exploit during the response[10][66].

Almost all BYOD implementation and adaption documents are mentioned that by adapting BYOD, the incidents will increase compromising devices, data leakage, malwares, data breaches, and unauthorized access are the type of incidents in IT community that will follow to the mobile devices. Enterprises and organizations should be prepared to respond to the incidents right away when it is observed; reporting and planning is required to ensure that the enterprise react to security breaches before the incident spread further and before the accident become unmanageable [23][10]. The capability of enterprise or in General IT environment is to respond quickly and effectively. In the Cisco interview, Henrik said that the biggest problem of risk securities is for the companies not to invest to the security development and not pay attention to the incident response (Cisco Interview). Having information about threats, tracking incidents, forensic tools, and application tests are the capability of BYOD incident response. Perhaps, the most important point of incident responder should be trained and well-verse on how to respond and where to respond and that all users should be trained to understand the enterprise policies and where they should not use the devices [10] for example, in the case of lost device the user should inform the IT admin to block the account and wipe the data on the device remotely or block the device (Cisco Interview).

10. Asset Management and Supply Chain:

This functional area tracks the assets in the enterprise and understands the supply chain from which those assets are obtained. This functional area is twofold: first, being able to account IT assets, and second, knowing where those assets came from, are they confidential level and whether they are doing what they were supposed to do. Asset management is an essential prerequisite for endpoint and server security controls to be effective. Asset management helps to ensure enterprise assets (1) are accounted for during their life cycle, and (2) made compliant with enterprise policies when they are put into service (for example, comply with network security, endpoint security, and other enterprise policies)" [10]. Asset management is also used after the asset is disposed and the enterprise data is disposed from organization properly.

The main task of asset management and supply chain is:

1) Knows the enterprise IT assets.

2) Manage supply chain risks through operation.

Keeping record of device, make a model, device owner, current software version, and install corporate applications are the objectives of ensuring that the staff follows proper procedures that are supported by various technical capabilities[10][36]. BYOD devices are owned by users that's why it's not counted as an enterprise asset and they are not under normal enterprise asset management and supply chain process. But there are some things that enterprise can mitigate security in this area. Enterprise should consider BYOD devices if they correspond or match to their purpose of needs, and enterprise needs to check BYODs devices if they are reliable to be entrusted with some high level of access like system administrations [10]. In this case, the device should be certified and can be tracked as an enterprise asset. For example, there are certain models of Android devices that are extremely vulnerable and they are not worthy to be used as a BYOD device, and the same cases for the applications. Malicious will seek out to exploit any security weakness in the technology supply chain, the vulnerability in supply chain technology can provide malicious to full house backdoors by the security issue which have not been consider by the organization [9]. The environment and devices should be

in the level of trust dynamically so that the organizations can fragment security models to provide inconsistent enforcement, isolated threat intelligence, and capable to manage the devices and product [9].

11. Policy, Audit, E-Discovery, and Training:

This area is a group of functions combined to oversight various security functions, including security controls to meet requirements, along with some secondary functions regarding personal security and privacy concern. For example, policy sets a strategy for all other functional areas. Audit periodically reviews all other functional areas to make sure that it complies with policies and prevents or detect control. This functional area includes training the IT staff and security personals to ensure to complying with the organization's security standards, and make sure that the users understand the tasks and awareness in order to perform their responsibilities regarding appropriate use of network, system, and applications[10][66]. This functional area is to control of enterprise processes and capabilities, and the management of programmatic and personnel issues associated with the process and capability deployment[10][66].

This functional area is probably the most important with respect to BYOD because when an enterprise allows BYOD devices to connect to their network they should have a clear policy for these devices. These includes securing all connection points, security policies, and technology limitation [10][66][15]. This policies are included in what business data can be access from devices; what business activity can be performed by the devices, what business activity is not acceptable to perform by device, what policy should perform to protect the data transferring to and from the devices and the data stored on the devices, and the policy and agreement with user for investigation on device when data breach is suspected [10]. The Auditing will periodically make sure that the above-named policy strategy is fulfilled and going well with devices and users and provides evidence that controls are effective. Training and educating employees about BYOD security, deployed solution, and enforcement of policies is crucial, all the device users should know and have understanding about companies BYOD security policies, and the consequences of violating this policies [34].

5.2 SWOT Method

SWOT is one of the most commonly method tools used for strategic planning. It helps organizations to gain a better insight of their internal and external business environment when making strategic plans and decisions.

SWOT means that Strengths, Weaknesses, Opportunities and Threats. The analysis is important for the BYOD security to identify the internal and external ability of the solution through the discovery of Strength-weakness and opportunities-threats. Strength needs to be on the line of being stronger while weakness needs to be covered in time. The BYOD vendors should take advantage of the opportunities and be prepared for the threats[20], [67].

- Strengths: Characteristics of the business or project that give it an advantage over others
- Weaknesses: Characteristics or features that place the business or project at a disadvantage position relative to others.
- Opportunities: Elements that the project could exploit to its advantage.
- Threats: Elements in the environment that could cause trouble for the business or project.

“In theory, SWOTs are used as inputs to the creative generation of possible strategies, by asking and answering the following four questions numerous times:

- How can we use each strength point of internal attribute to achieve the objective of the organization?
- How can we identify the weaknesses that are harmful to the achievement of the objective in the organization and how to stop them?
- How can we exploit each Opportunity and use the external conditions to the achievement of the objective?
- Threats are the external conditions, which are harmful for the organization, how can we defend them?

It is expected that this approach will provide more accurate information for strategic planning as it generates prioritized SWOT factors based on the user's perception[68]".

Today's business environment and economic competition is becoming global, customers and technology use are changing rapidly, these changes had forced the organizations to find ways to build proper strategic plans and right decisions to develop effective business and influence the competition. These business environment technology developments have a lot of risks and impact, which influence economically and affects life cycle as well as manpower. BYOD is a phenomenon which uses modern technology to build strategies and policies within an organization or enterprise to help them correspond to their employee's demands about bringing their own devices for business purposes and for the benefit of the organizations. As had been mentioned, SWOT analyses will support business maker in building a proper strategy in achieving the objective goals, that's why SWOT analysis is used to analyze BYOD strategy in the risks and securities perspective [20].

Strengths*:* The strongest point are the vendors of application and technology developers to satisfy their users, they testify the applications and update the applications to dispatch the vulnerabilities for example, MDM and MAM. The employee's knowledge and familiarity to their device, because of having prior experience means that they can manage their devices better. Smartphone's cellular data connection technologies 3G, 4G, 5G are strength of BYOD security[23], because the connection is fast and high capacity of data transportation and capability of encryption, decryption mechanisms. EMM enterprises can provide a freedom for employees while maintaining security and control, they still can have single-click access over any other networks, and unify their apps store on the devices as they want [7], and MCM in addition to MDM support IT managers to check app-by-app approach to the security control, in this way IT cost reduction occur by making it easy to work securely, seamlessly across any type of device regardless of who owns the device, and the most important point is wiping lost devices data option [7].

Weaknesses*:* There are numerous challenges involved in security process of BYOD, the inconsideration of employees and not following the policies and instructions of the enterprise is one of the top priorities of weakness [Cisco & UNDP interview]. Malicious apps, having certain number of applications installed on the devices increase more risks because of possibilities of holding malicious or security flaws, which the device applications are not under organizations' control while the organizations enable employees to bring their own device [37]. App vulnerabilities means the apps developed by organizations which have not been tested and are vulnerable to the malicious; it will be risky to enable them and used to access to the corporate data because it may contain security weaknesses [37]. Because of employees carelessness in visiting unknown cites, mobile application gap, navigating in social media applications, leaving the applications as logged in without logging out on their mobile device are all weaknesses of the enterprise which give an opportunity for data to be compromised or being installed malwares [Cisco interview][24]. The weakness is that a very small device can cost a very big problem for the organizations which are implementing BYOD, because those devices brought into the company network creates a loophole through which malicious can follow [69].

Opportunities*:* BYOD phenomenon has been successfully applied to many enterprises and organizations, different problems have been covered and solved [Cisco & UNDP Interview]. There are different kinds of software defenses such as antiviruses, firewall, etc. to protect the system and devices, existing multiple technology solution for BYOD, educated users and providing them the instruction or guiding them on what to do and how to be protected. Enforcing the organizations security policies to protect the device applications and the network is also a helpful way in preventing security breach.

Threats*:* The threats are creating security risks on the business to enterprise, they are external factors and harmful; it includes external malicious persons that aim to harm the business data and infrastructure, online criminals, and sometimes, former employees that may deliberately or unintentionally transmit, delete or modify the corporate data for their personal benefit or due to them lacking appropriate training[23].

By allowing BYOD, different threats can appear, such as losing of mobile device may cause data to be lost in it, and may also allow unauthorized users to access to the sensitive data on the device or it may use to compromise and gain access to the organizations resources [70].

A multi-manufacture producing mobile device which have diverse operating systems, with various OS devices concerning the device itself can also be considered a threat. The security faces difficulties since corporate confidential data can be leaked as a result of incapable device management [24]. Mobile device connections from wireless public WiFi and Internet through corporate networks significantly increase threats to sensitive data [32]. There are set of mobile device vulnerabilities in which their key assets are defined by considering all aspects of security, including physical weak points in the access points, technological gaps and insufficient organizational policies, employees carelessness, and device lose and stolen are all threats in losing sensitive data or data breaches to the organizations confidential business data [23].

The following table presenting the dimension of SWOT analyses in relation to helpful or harmful with internal and external factors.

	Helpful	Harmful
Internal	Strengths: ● Software and device vendors ● New educations, innovation ● Technology acceleration ● Policies, Data encryption, Remote wipe, Password protection	Weaknesses: ● Employees ● Policies ● Applications ● Wireless access
External	Opportunities: ● Different kind of technology ● Software protection ● Employee training ● Smartphone's cellular data connection (3G,4G, 5G)	Threats: ● Multi manufactures devices ● Multi OS ● Collaborative network ● Applications

Table 2 SWOT Analyses of BYOD Risks[68]

The table above shows the SWOT (strengths, weakness, opportunities and threats) analysis of the BYOD strategy in the risks and securities perspective

5.3 Consideration for BYOD Adoption

As we mentioned before, as well as through the researches pointed out, BYOD phenomenon will bring serious security risk and threats to the organizations.

This situation creates dilemma for organizations' and enterprises' IT department in adopting BYOD, in which they need main corporate data security, while enabling more devices and functionality. That's why they are under pressure to find a balance between employees demand and mobile devices platform diversity and security requirements.

In the guidelines of security mobile devices NIST [8] placed that, mobile devices should implement the following three mobile device security to fulfill minimum requirement security (Device integrity, Isolation, and Protected storage).

Device integrity is when there's no corruption in the hardware, firmware and software of the device, which means there should be evidence that the device can be trusted by a relying party. Isolation is preventing unintended interaction between private and business information on the same device.

Protect Storage is a protection of confidentiality and integrity of sensitive data on the device while it is on use or at rest. And NIST in the guideline for managing the security of Mobile Devices in the enterprise [14] states that before designing and developing mobile device solution, organization should develop system threat models for the mobile devices and the resources that are going to be accessed by the mobile devices. At the same time the guideline [14] pointed out that the major threats organizations should concern about mobile device are the following:

Lack of Physical Security Controls, because of using mobile devices in a different location it is out of the organization's control, and as well as often transported from place to place, that's why it is much more likely to be lost or stolen than the other devices, so their data is riskier to be compromise.

The use of Untrusted Mobile Devices- many mobile devices particularly those that are personally owned are not necessarily trusted, because most of them lack the root of trust feature.

The use of untrusted networks; mobile devices normally using a non-organizational network for Internet access and organizations have no control over external network. The communication of mobile devices includes WiFi and cellular networks which those systems of communications are vulnerable to snooping and it puts sensitive information transmitted at risk of leak or compromise.

The use of Untrusted Applications: mobile devices are known as easy to find, attain, install, and use; third party applications from mobile application stores which a security restriction is not on place. Organizations should plan that downloading and using third-party applications should not be trusted by users.

Interaction with Other Systems: mobile devices may interact with other systems for data exchange and storage, such as mobile device to desktop, Laptop to-wireless, Mobile-to-mobile, using one mobile device to provide network access to another device, remote access interaction like automatic backup on cloud based storage solution. When all those component and activities are under organizations control the risk is generally acceptable, but when one or more of this component are external, it will bring a security risk, for example connecting organizations issued mobile device (smartphone) to your own laptop or in public wireless connection will bring the organizations data to risk.

The use of Untrusted Content: mobile devices are capable to use untrusted content which other type of devices generally cannot counter. For example, mobile device is capable to view and proceed to Quick Response QR codes which can translate the code to text and typically a URL, so the malicious QR can direct mobile device to malicious website.

Price Waterhouse Coopers (PWC) in its report about BYOD agility through consistent delivery [12] mentioning that security of data is paramount, security should cover every aspect of access to the network, data, and applications they consider to isolate corporate data from personal data. And PWC believes that the weakest link in BYOD security is often the users but liability often originates at the top, that’s why the leaders pose the

greatest risk because they have access to the most important company's information. PWC mentioned policy and strategy is another important aspect, CIO should implement a very strong set of policies and enforce it to govern employees use.

Citrix in its explanation of best practices to make BYOD simple and secure states that[7], the ideal approach for BYOD is enabling completely device independent computing, and protecting enterprise network, supplemented by a secure file sync and sharing device. And Citrix express that IT can simplify management and reduce costs while they allow people to work seamlessly across any type of device, regardless of who owns the device, and empowering people to work easily. Bottom-line is that Citrix's considers that the best practices for BYOD is simplicity for people and effective security, control and management for IT, and provide secure access to data and applications in term of users. Eligibility of BYOD in organizations should be allowed to determine who can use personal device in the organization and privileges, and a requirement for certain type of roles [7]. The main requirements of Citrix in adopting BYOD are; empowering people to improve productivity, collaboration and mobility; protecting sensitive information from loss and theft; reducing costs and simplifying management through self-service provisioning; and finally, simplifying IT by deploying apps for use of any device.

The analysis paper about BYOD security framework [4] considering to the security risks points out that enterprises need to ensure that the data is encrypted while at rest on the device or in transition process to guarantee confidentiality, verification and authentication and it must be on place before data access granted, the access permission is provided by hierarchy which means employee can have access data from enterprise based on their position, isolation between personal data and business data and applications. The device must be enforced to use a complex password, the system should require a minimum configuration by employee and it should be cost effective [4]. Concern to BYOD adoption strategy, different business will have different expectation from BYOD adoption scenarios, every business needs BYOD strategy, even if the intention is to deny all device except IT approved devices [6].

The following Figure shows different BYOD adoption scenarios:

Figure 17 Different BYOD Adoption Scenarios [6]

Consequently, it's in the author's interest to stress out the assumption of some considerations for BYOD in this research to find out the right balance between end user demands and organizations' diversity and security requirements.

In response to the abovementioned, an enterprise must ensure that the BYOD framework meets the following basic security requirements.

- To guarantee confidentiality the data must be encrypted while stored on device or during transmission to prevent unauthorized people to access.
- Verify authentication from the requesting party before data access is granted
- Employees' access to the enterprise data based on their, position, permeation, and privileges
- The communication between BYOD devices and enterprise server must be secure
- BYOD must isolate employee's personal applications & data from corporate applications & data.
- IT administrator should be able to wipe or block device in the case of lost device, or non-compliance to organizations policies.
- Minimum requirement of configuration by employee (users).
- Cost effectiveness (the cost of adapting BYOD must be less than company owned device).

- Available and accessible at any time and any where
- Capability to enforce policies.
- The system will include different factory devices and OS's.

5.4 Chapter Conclusion

This chapter presented the theoretical framework to the research idea. Theoretical framework would help to provide the basis to explain the fundamental problem and would help to point out where the troubles are and why they were the problems.

Chapter 6

6. Case Study & Interviews

Today's BYOD movement has work force implications, as employees consider using their own device for work and believe it will support them ahead in their careers, which encourage companies, organizations, and enterprises to be flexible because their markets will grow and there's flexible attitudes towards working hours. This behavior will not only be the future of mobile high growth, but it will also dictate which market structurally will benefit most from this BYOD implications [71].

6.1 Cisco's Interview

In relation to my research of BYOD security challenges and risks, I got an opportunity from Cisco to hear about some practical grounds through my interview with them on 8th of July 2016. For the detailed questions asked in the (Interview) please refer to Appendix1 and (recorded Interview in Audio Cisco Interview).

The interview was made with Henrik Staer, System Engineer manager (director), who had been working for 17 years in Cisco and Per Jensen, the Consulting System Engineer who had been with Cisco for 22 years.

Cisco started to use BYOD in their company 5 years ago (Said Henrik 2010 -2011), Cisco's definition of BYOD is a possibility for employees of certain organizations to carry their own mobile device (phone, tablets, and laptop) or whatever kind of device they have and get more access to company's resources and they just normally get internet access to do it. The reason that BYOD is becoming relevant now is because of the change in work life balance and because devices became handier which made it possible to manage a private device as a working device for the company and we can have the integration between android and apple into organization's infrastructures. Mobile devices are powerful enough to carry private and business applications, flexibility and creativity is also the other reason for having BYOD and it is catered for work life balance perspective.

Cisco believes that companies' own devices are not flexible and cooperative enough for employees. Henrik said, when he was working for TDC he had a company's laptop it was so restricted he couldn't even do a simple update and even couldn't browse on the internet, even his earlier days in Cisco he was under IT department control, but now with BYOD it is so much flexible, productive and multipurpose used.

On the questions about security risks, he said that there are unavoidable security risks, but IT department has BYOD security policy and they have a certificate installed on their device which is a system that can recognize if the device belongs to Cisco's system or not. They also have different policy for the different devices as a hardware and software. In the Cisco's business policy server, they integrate MDM technology with their server access control and all employees have agreed to the protocol that when something happens to their device or if the device is lost they report to the system so the system's robotic will wipe all the data and applications located on the device.

Per and Henrik believes that the on the scale level of 5, BYOD security is 4 out of 5, and they have no problem with it, as mentioned above they have implemented a mobile device management technology to control each devices security. Cisco's BYOD system allows two types of hardware and software such as android and apple's iOS as employees' own device. The registration process requires each employee to register and have username and password when the user connects to the system; they should provide username and password, when it is authenticated, the system will certify the device then register it in the system. The certification will be located and stay on the device so the device will be recognized by the system and give authentication anytime it is connected. One of the biggest security problems is, if the users don't deploy additional security policy. The challenge for the IT department is deploying additional security because of extra devices connected to the system. In relation to the employees' biggest risk, the solution is that employees should follow the rules in being mindful of visiting strange sites and links. For employees to follow the rules in security policy, the company should guide and educate them and make some sort of warning when they have acted against good behavior. The biggest challenge of BYOD security that Cisco strongly considers for the future are two things: one is the company will invest enough in security and second is being more aware

of how the people behave when they access the Internet especially if they are connected to the system of the company. Cisco categorizes the security in to 3 steps before during and after, and the biggest risks of BYOD are the things we don't know are risky, the creative malwares are riskiest because we don’t know what they do.

Cisco’s authentication system is multifactor authentication system, for protection, they use firewall and intrusion detection system with anti-malware system.

About recovery, if the device is lost or given away the system will wipe the data from the device and when there is a new device it will start the same process in the registration and authentication to be recognize by the system. About the future of BYOD, Cisco believes that it will be used by 20-30% of the companies in Denmark in the next 2-3 years.

The main purpose of using BYOD for Cisco is to attract younger people, to make Cisco modern and innovative company's work form and to create the best work space for employees, they also believe of flexibility will increase productivity, comfort, and employee’s efficiency. For international company like Cisco which concerns with people working in different working time zone, it’s like always working whole days because of time zones, sometimes they correspond with each other even while others are sleeping in the other part of the world. (Productivity, flexibility, and attracting place work with flexible work life balance these are key point of using BYOD).

In relation to BYOD cost and saving money for the company, Henrik admitted that the company of course saves money by adopting BYOD, in the sense that the company doesn’t need to provide for each employees’ devices and the employees will be more productive by working more hours (since they can also do their work even while after office hours) eventually, without being paid extra by company and it’s more flexible for the employee to choose the device and operating system that they are used to which give them the upper hand due to comfort and ease and make them more productive and creative in a sense because they feel like they are in their own element with their chosen device.

The BYOD’s market opportunity is massive, Cisco also has massive market opportunity by selling infrastructure, hardware and software and security system. The last five years

has been the fastest growing market for Cisco mobility of BYOD. Cisco and Apple have a cooperating work based on integrating apple device into their enterprise for customer to collaborate telephone integration and video integration and stuff like that.

6.2 UNDP's Headquarter Interview

To have an overview over organizations vision on BYOD, I got opportunity to have an interview with Moe Kyew the global ICT specialist, in 19th of October 2016 and the manager of global connectivity support at the UNDP, he is working for 4 years in the UNDP headquarters' department in Copenhagen

Moe defined BYOD as, "one bring his own device to perform the work better, and one bring his own device that familiar with all tools inside so that one can perform job better and faster, especially software for the work environment. Because when the office issues the device its bit difficult to load the tools that you need to work." Especially in his case networking field, he need different tools to the asset, to the router, and to the switch. There are lots of networking devices like console connection, ssh, telnet and sometimes he needed an additional software on the laptop, sometimes he needed special tools like SNTP and some simulator to monitor traffic. All these tools he needed to do the work in his laptop, which is hard to imagine if it weren't a more portable device like that of organocation's issued device. If the office issues the device, sometimes it comes with the global policy defined by the office which has a definite level of used and not used tools. Sometimes, for even just installing software to work better, you are not allowed to do it freely and immediately, one should go to the office to install such tools and software or ask for the permission to install.

In answering the question of why do we need BYOD when we already have company issued device, he said, it all depends on the type of job you have and how you worked with it. For example, for their staff to work on the office they issued the laptops and everything install on it. He thinks it's fine like that they have everything they need and it's easier for company to manage as well. But if company can customize an image with all those tools, then they don't need BYOD which is one other concern, he said. UNDP doesn't have a global UNDP policy yet but few offices have been using BYOD. In the

office, they don't use BYOD as official and they don't have any control mechanism, not policy management and not authentication, although, they provide access control to those who bring their own device but not for work purposes. I can observe that they have an internet access (Figure 1 chapter 1.1) connectivity flow for personal devices. In the answer to my question, what would be the reason if UNDP will adopt BYOD? He said, there are different views, pros and cons, and risks and cost saving but the advantage that he can see for the UNDP in allowing bring your own device, is they don't have to manage this asset anymore. For example, if the office issues a laptop, it must control that asset which it should be put in the asset management system for asset depreciation, calculation asset disposal all those things to be done in the background. These issues are only to manage and make sure that asset will not lost; background logistical issues.

He said almost everybody brings one device with them to the office and they set up an access to have connection. He said, if they will implement BYOD they look at some business cases to know what will be the benefit, but he is not sure in terms of economic benefit. But, Productivity and flexibility are two benefits of BYOD, he said because sometimes even kind of keyboard is an issue for worker to work on and somebody will do the work of half an hour time will take 2 hours with the matter of different kind of device. But if employees have their own device they will finish from those headaches. In the question about risks, he thinks are very heavy and serious is if you don't have a proper mobile device management and security control mechanism, it can cost millions of dollars. (min 33) In case of security, he believes there are risks even with company owned devices, for example, enterprise management system and everything is in the cloud, the financial guy has a permission to all the money transfer and bank details, so if his credential details leaked, someone can login and make damage that can still happen without bring your own device, but with BYOD the risks are higher. Those risks can be controlled by mechanisms (manageable risk) like security policy and multifactor authentication mechanism or different level of authentication mechanism to make sure it's the right person and information has not been leaked, and wiping mechanism in case of lost device with information. So, he thinks that we definitely need control mechanism in BYOD because the risks are higher.

Moe believes that the on the scale level of 5, BYOD security is 3-4 out of 5, and most of the risks are manageable by policy and control mechanisms like mobile device management technology to control each devices security. In the case of compromising device, they have the case which one of their laptop had been compromised and the hacker were asking for money to release the data in the laptop, but because there were not sensitive data on the device and they had a backup, they just wiped the laptop and reinstall again. Moe believes that the risks are on both sides; user side and company side, the risk for company is that the information will be in risk to leak, and in the user side because the user give permission to the company to control his device, all user's secret data and credential information is not confidential anymore. The biggest challenge of adopting BYOD in his opinion depends on how strong is the policy. If the policy is strict the challenges are more. But now there's not much of attention to the users, they can have their device and do what they want but they don't have access to the share drive and they are not allowed to print, but they have all other facilities tools like emails, office, and so on. In the term of confidentiality, integrity, availability, he said because it is a transparent organization they don't worry about confidentiality, but they are more concern to integrity and availability. They are just testing BYOD now and they are not forcing any control mechanism now that's why the confidentiality will be in the risk, and at the same time they are testing MDM to understand the technology behind this, productive or not, losing information or not. Once they understand the risks they are taking in consideration to use it or not. There are a lot of risks with BYOD but in different levels, but the access is very risky because one take personal device in everywhere and connects to the different access points which will be risky to infect device with malware and bring it to the organization's system. At the end of the interview, he admits that there were very good questions and included a different scenario of BYOD, and he thought it was a very interesting discussion. For the complete recorded interview please refer to the audio file titled UNDP-Copenhagen-Interview.

6.3 Using BYOD by UNDP in Bosnian-Herzegovinaas a Case Study

UNDP stand for United Nations Development Programme at the center of UN organization to help people worldwide in the case of natural disasters, catastrophes, disease, and to reduce poverty. UNDP is based on the merging of United Nations Expanded Programme of technical Assistance, created in 1949, and as UN's special fund established in 1958 which has a local department in different countries [72]. The main headquarter is in Copenhagen, and it has a department in Bosnian-Herzegovina with 230 employees.

After having an interview with Moe Kyaw in the main department in Copenhagen about their adoption of BYOD, it turns out that they haven't adopted BYOD solution in the main office, but he introduced me to Ognjen Krstulovic who is the head of ICT unit in UNDP Bosnia-Herzegovina where he had been working for almost 20 years and they adopted BYOD in their department partially. This case study is the result of skype interview on 20th of October 2016 with Ognjen Krstulovic. UNDP in Bosnia-Herzegovina has implemented BYOD only for mobile phones, the main reason of implementing Smartphone BYOD is because they are used to buy mobile phone for their staffsand then they offer the staffs an option that UNDP don't purchase the device for them, but they provide an eligible refund for using the phone that they buy for work. After asking their employees in a survey, if they provide the eligible amount of money that UNDP budgeted to buy for company own device they will give to the employees, then they will be the one to choose and buy the phone and they will pay the overprice by themselves. In the beginning 20% said yes to purchase by themselves because they expect to be supported up to 250 Euros but when they knew it's only 100 plus, they realized UNDP can buy them a better cellphone with this money by the contract. UNDP organization provides €100 to each staff and provide a sim card, the survey's results that 15% of the staffs agreed to the UNDP's suggestion, and they agreed that if the employee leave the organization within one year they must return the €100+ to the organization, but above one year's usage on the phone in the organization even if one leave the organization should not return the support money (one year breakdown). But in the term of computers, they don't allow employees to use their computer for work purpose, but they configured a wireless access to those who bring their

laptop to work in the office and very limited access to the organization's information. The reason UNDP decide to provide the employees with €100+ Euro and sim card for mobile are the following:

1- Their budget per employee to buy mobile device is only€100+
2- Employees' satisfaction, as users might be happier to use the device that they have picked up by themselves rather than what UNDP give them.
3- Ease of maintenance or much less maintenance of the devices. If, users are responsible for the management of the devices
4- The user's efficiency and satisfaction as the user would be much better to use equipment they choose because they are not accustomed to the company device.
5- UNDP's less maintenance if the users are responsible for the management of the device, or servicing them, or they get by themselves another one if its broken
6- UNDP cannot pay full price of buying mobile devices based on staff's choice (Economy reason).
7- The assets management by the IT department will be easier.
8- And in particular related to UNDP is fertile organization most of the system is web based and centralized, so UNDP don't have to do so much on the client equipment to install or updating etc. in relation to the ERP, Internet etc.

But on the other hand, he mentioned some negative side as well. UNDP should have a monetary support to buy equipment, and they spend the same amount of money they used to purchase mobile devices, that's why in the case of money they don't have that much gained. And in some cases, it's easier and cheaper to buy company owned devices with the agreement with device provider in a reasonable price and two years guarantee to fix or replace them in the case of defect.

Related to BYOD adoption, UNDP in Bosnia-Herzegovina adopted BYOD before they have done a global policy and it's a basic partial access adopted policy (Figure 19, 20), which users have an access to the internet, and very limited access to organizations data, like access to ERP and email system and calendar with limited privilege from the employee's mobile devices On the other hand, at the same time, they also paralleled 60% of the staffs who use organizations' owned device, so it is a

kind of Hybrid approach. In UNDP's global policy, it is not allowed to supply users to purchase their own device and not this kind of monetary subsidies, but in Bosnia-Herzegovina they did that to achieve within a certain period (within 2 or 3 years) to stop buying cellphones. They will only provide sim card and telephone numbers so they can purchase any kind of cellphone they want by themselves.

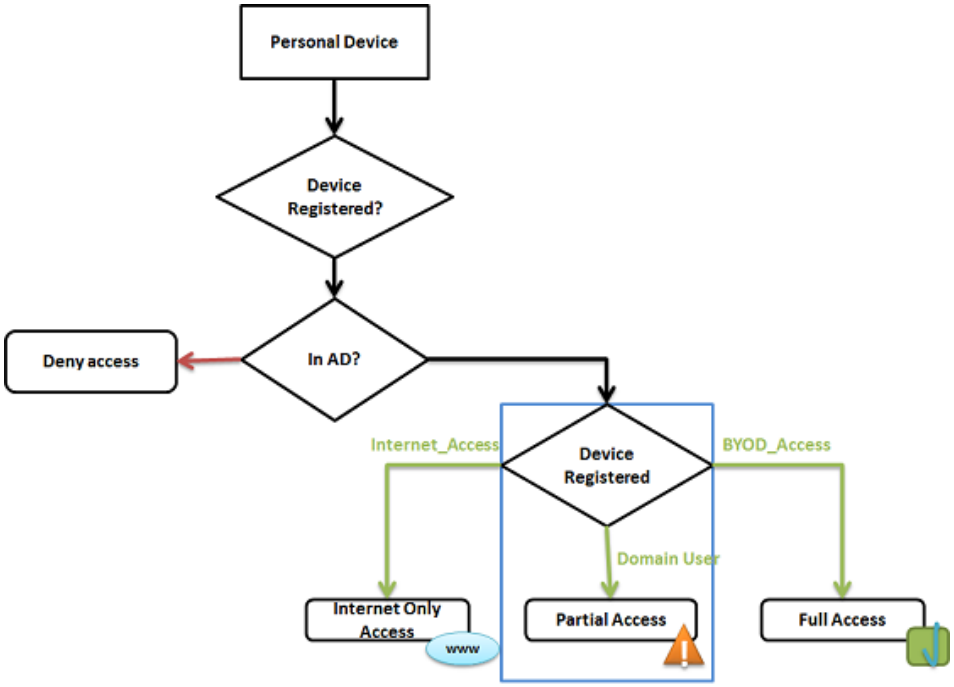


Figure 18BYOD Topology in UNDP Bosnia-Herzegovina

The figure above illustrates the topology of adopting partial access BYOD in Bosnian's UNDP department

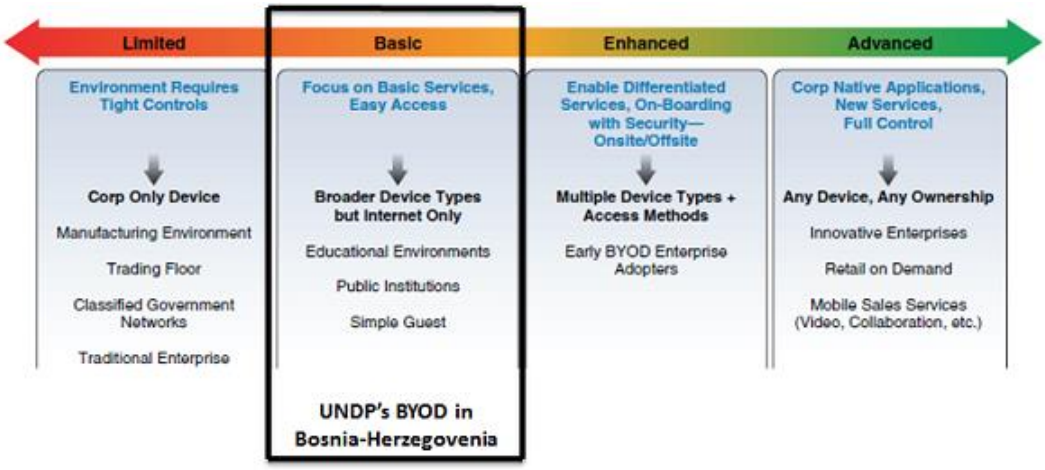


Figure 19 BYOD Adopted scenario in UNDP Bosnia-Herzegovina[6]

The figure above illustrates BYOD scenario adopted partial in Bosnian's UNDP department

Related to the security issues, Ognjen Krstulovic said we have a fertile situation where Bring Your Own Device is not as dangerous as it might be in some other companies. But most of the threats of BYOD are covered with policies, not with the actual security measures; the only thing we should be worried about is how the user can be authenticated to our central web based system. And this is, if you have a good authentication system and followed to the industry standard which UNDP probably does. If the user can connect to the ERP system, it doesn't matter if it's in the café or at home or where ever. But the greatest threat is what happened to the data on the devices, this is hard to control by any kind of tools, and they don't know what the people do. In the case of the device lost or stolen UNDP is capable to wipe remotely the device, and even if the user want to remove data from the devices they can also do it, and they do it through the application called office365., It is convenient to have the office365 they don't need to implement any additional software management. And it is interesting that he said he will not invest in any security measurement and security development area, because it wouldn't change that much; UNDP can cover the threats by significant policies instead of tools, UNDP can do that maybe some other organizations cannot, because if you chose to implement tools to manage privately owned devices, it would probably cost you as much as managing company owned devices. For the complete recorded interview please refer to the audio file titled UNDP-Bosnia-Herzegovina-Interview or Appendix 4.

6.4 Chapter Conclusion

Chapter 6 presented different interviews with companies about BYOD. There are tens of cases, which used BYOD solution but research cannot be done in all of them, besides, the semblance of the cases make, it is useless to study each of them. Despite of that, it was my choice to research different cases in the practical way with different companies; however, an interview with more companies to hear their argument about adopting BYOD, and the benefit of it in their perspective is favorable with the depth of my study. Therefore, different companies were chosen to make the contrast and point out the effectiveness of BYOD both theoretically and practically, in the case of the interview with Cisco Company in Denmark which used BYOD for cloud solution for enterprise, and teaching school for online teaching. Those companies and organizations are less sensitive of business data related they are more embracing BYOD. UNDP as a public transparency organization is one of the less sensitive organization for their data to be shared, but they are more focused on employee's satisfaction, productivity in the organization, and device purchasing cost saving by implementing BYOD.

Chapter 7

7. Analysis

The research conducted with the theoretical framework and literature review with the use cases and company's interview. In this chapter, I'll try to narrow down this research and point out the risks associated with BYOD, the trend of this phenomenon and its economic impact.

7.1 Threat Model of BYOD

BYOD phenomenon is about employee's choices to bring their own device to participate and conduct their work anywhere and anytime they want. This phenomenon needs mobile devices. Mobile devices have vulnerabilities and security problems; these security problems increase when the devices joined the organizations networks and uses two types of applications for different purposes (Private, business) on the same device. That's why typically mobile devices need multiple security mechanisms and support to undertake the security issues[73].

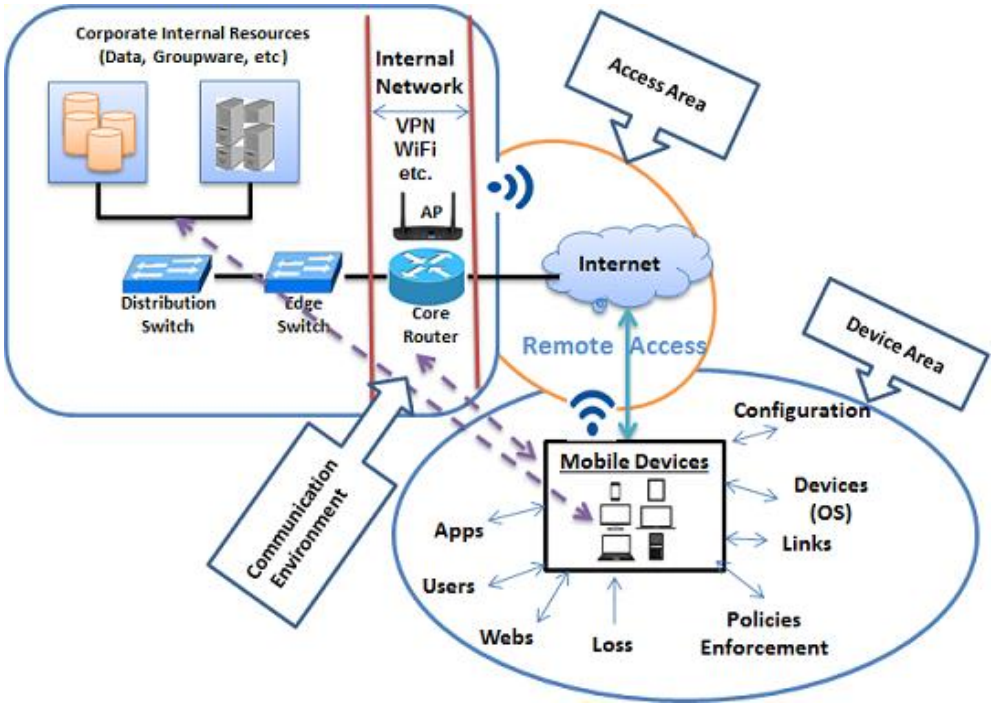


Figure 20 BYOD Threat Model [Author]

This figure shows the BYOD Threat Model Overview, the model shows how mobile devices connects, where will access's, and what will create threats.

The above figure shows different objects related to adopting BYOD regardless of different scenarios and topologies mentioned before, there are still threats to leak the data or compromising devices. The figure illustrates that threats can be divided in three areas; the device area, access point area, and the communication environment. Access point can be a threat if the authentications are not strong enough and the password preferred to be a complex password. The organizations should have a clear strategic and policies to adopt BYOD.

In the communication and transferring of data; downloading applications can be threat, by downloading malwares or vulnerable applications infected by malicious code, transferring a plain text is very possible to be read or change by malicious.

The device area is the highest threat and risk, because the mobile device can be physically contacted, like lost/stolen or other facility mechanism such as applications, user itself, OS's and manufactures vulnerabilities, and visiting different links can be threat to compromise mobile device or be used to reach the organizations' data.

7.2 Security Analysis

Since daily life is more interactive with digitalization and dependent on computer and information & communication technologies, computer criminals and malicious are also trying to interrupt and misuses this area, that's why there are lots of threats and risks.

Based on literature review, and interviewing different organization's IT expert, and my knowledge, using BYOD will increase security risks. For example, in the traditional enterprises network communications and company owned device used, they are secured and controlled by the organization, to communicate with internal and external network devices and assets. There are mechanisms to protect and secure the endpoints; the enterprise has total control on the asset and end user's device. There is no such thing as perfect endpoint security, but by adding employees own device as an additional

enterprise endpoints which are not owned or managed by the organization, it will create risks and threats to the organizations. As mentioned in threat model above, there are three areas (the device area, access point area, and the communication environment) of mobile device used in the BYOD that should be of concern which will bring risks to the organization. Authentication is one of the risks in using employees owned devices, because employees owned devices are vulnerable to malware and malicious apps. Malicious Apps on devices will attach organizations data or compromise device. The access will be another risk, while mobile device is connecting and accessing organizations data remotely; this will bring risks because it can be connected from public/private access point in which these access points can be misused by malicious for compromising the accessor's identification or data. Another risk is when mobile devices used for work purpose, it's very possible to save sensitive data and applications locally on the device and because mobile devices are small and carried around by user, it is possible in a way or another the device will be (lost/stolen) then the unauthorized person can possibly access the data located on the device. Downloading untested applications by users will bring risks to the organization's data and application. Users are one of the highest risks, because it's the user who has the control over the device. If the user is not aware of protecting the device from physical contact by stranger, it's possible within minutes to add virus in the devices. The user is also responsible in updating on time, if the user is not aware of updating the applications or device software it's possible to create risks to the organization; the user should follow the policies and be responsible in visiting unknown websites which is infected by malicious code, although this is un-avoidable at times, because the device is used for private purpose as well. Not aware of protecting access identity like username/password in the public area may make it possible to steal the identities to be used by unauthorized individuals. Fired employees will be another reason for corporate data to be compromised; disgruntled or fired employees may retain data on the device even after they leave the organization. Those risks can cost to leak the organizations' information and sensitive data and may be compromised.

Even though, there are several BYOD security solutions in the market currently, these solutions are either vulnerable to many security threats or require modifications to patched with mobile devices' OS. The following figure is my proposed BYOD security

architecture; Figure 21A is MDM technology used to control the BYOD devices. In this architecture scenario, an MDM agent is installed on employee's devices (how it can be install on the devices? It has been explained under MDM technology) and MDM server is managed by IT administrator. In this scenario, it will create an isolated container on the devices, this container will hold all the data and applications and they will be encrypted. This container will hold only enterprise data and applications but employees can install other applications in the private space, which are not corporate ones. The corporate applications are sent by MDM server as a list and can be installed in the container. The applications outside the container are not allowed to communicate with applications inside the container[74], but the applications within containers will arrange the communication to achieve requirements by using IPC (Inter Process Communication). With the applications list, MDM server will also send security policies including the password, remote data wipe mechanism, and how many times password fails attempt would be allowed to the MDM agent. If the policies are violated, based on the policies requirement and enforcement, the agent will send a report to the server, the server will analyze the report and send a command to the agent to control the device [4].

The Figure 21B shows a scenario, which can be different from the similar architecture, for example if MAM technology will be used instead of MDM the scenario and process is almost the same but MAM can install and remove the apps on the device remotely and update the system without the permission of the owner. On the other hand, if MAM wants to remove or wipe business data from the BYOD devices, it is capable to wipe only the applications and data related to the enterprise but the private/personal applications and data will remain on the device. Whilst in the MDM scenario, the agent will wipe the entire data and applications of the device private and business. The following figures will illustrate the scenarios:

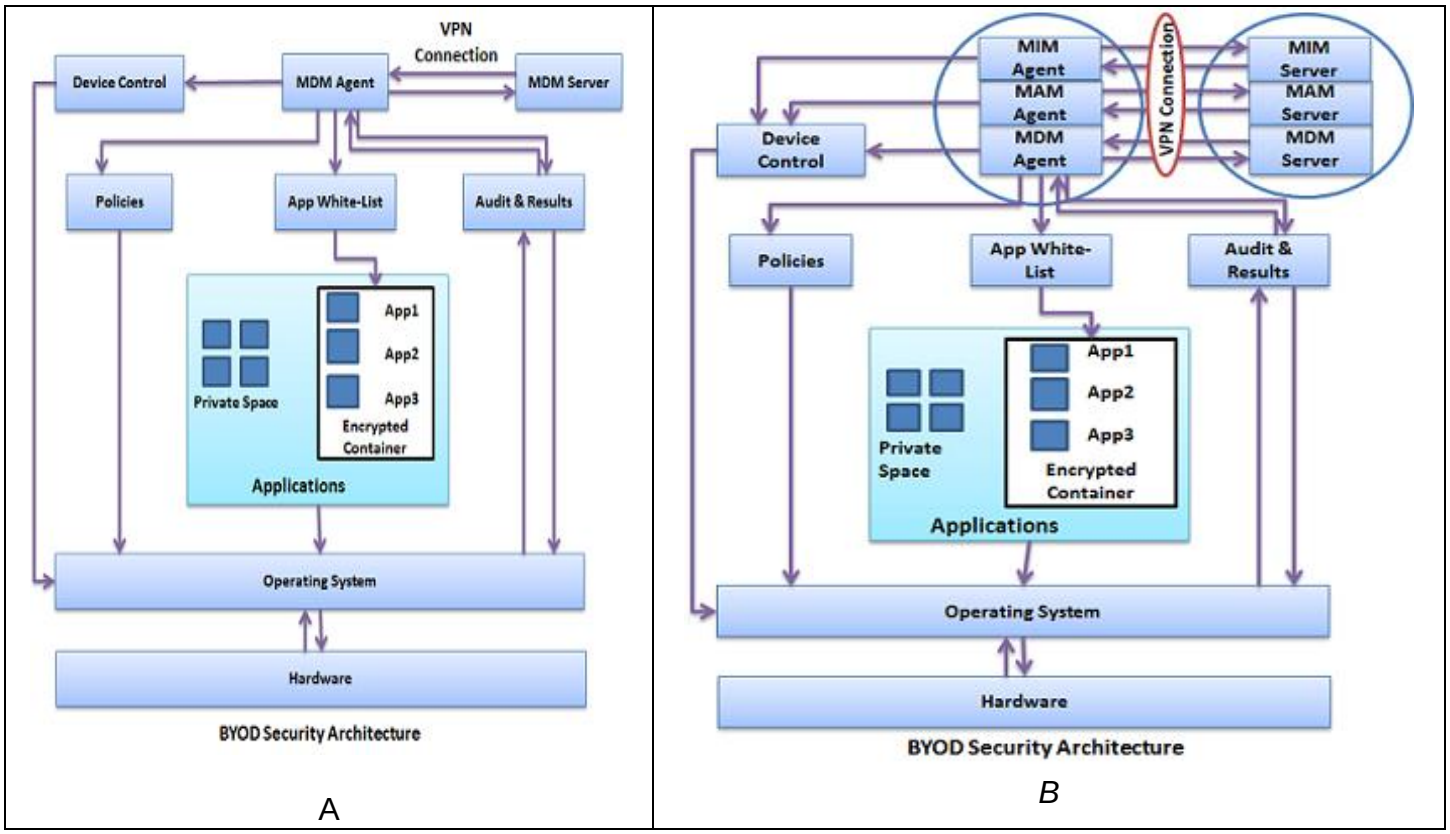


Figure 21 BYOD Security Architecture [4]

This figure shows the BYOD security architecture overview. Figure B shows the scenario which can be different from the similar architecture, Figure A, for example if MAM technology will be used in state of MDM scenario, the process becomes almost the same but MAM can install and remove the apps on the device remotely and update the system without permission of the owner

The above architecture and mechanisms will bring some challenges for the IT admin in imposing the circumstances. Remotely controlling the devices will be a great challenge to be fulfilled; data management on how enterprise will separate private data from corporate data on the same device is an exciting challenge. One more challenge is how organization can encourage employees to follow the policies (policy enforcement) and convince them to be cautious in using the device in the public place such as, protecting access identity, authentication. Enforcing policies on different manufactured devices with different OS will be also a great challenge.

7.3 The Role of Enterprise and Different Technologies

Enterprise has been focusing on the 11 functional areas to control the risks and threats to secure the end device, each functional area defines a solution resulting from enterprise's observation and analyses based on devices vulnerability and devices threat elements. The technology solutions try to cover those functional areas to correspond the security level of protecting enterprise endpoint mobile devices, that's why different technology solutions exist in the market. For example, by using MDM solution enterprise can fully control the mobile device as mentioned in (section 4.1), but this solution cannot provide the users privacy confidentiality, because the user should agree to give full permission to the organization to control the device, then the device will be treated as a company-owned in concerning to control mechanism. On the other hand, if a contractor work for the organization and use his own device to enforce the policies, the contractor must agree that the company control his device with MDM solution, but when the contractor leave the organization for any reason then the company's remote wiping mechanism will wipe the entirety of the data in the device. This is because MDM is not capable to separate private and company's data. But this problem has been solved in MAM solution, because MAM can manage private/company data on the device by using containerization which separate enterprise data to control and leave personals private data and applications alone. More details (section 4.4).

The following table provides the Pros and Cons of different technologies used by BYOD.

Technology	Pros.	Cons.
MDM	Secure for device data and applications, covering most of threats, fully controlling the device, vendors take a responsibility to the functionality example IBM provide MaaS360 MDM solution, centralized, simplified solution which allows businesses strictly control mobile devices	It is costly, Needs a strong policy strategy, there is no user's privacy, not sure of all device fabricant and OS's that's why it needs device vendor's corporation, software is a bit heavy-handed and restricted for users. Needs MAM deploying mobile apps securely to the potential users, lack of trained IT staff to administer the system, it is possible some device laptop and

		PC to prevent MDM system, there is not a one-size-fits-all system
MAM	Concentration is more on the applications, more user's privacy, giving the company flexibility to support a diverse device ownership environment, deploy the app safely to any user's device and effectively enables the organization to dis-tribute the apps to any user throughout the extended enterprise including those uses MDM. enable access and authorization control over cloud-based resources like cloud-based CRM for mobile devices	Not strong for remote installation, it needs MDM to distribute secure policy managed applications to device, expected to be a feature for MDM in the future, Limitation regards to access control and heavy focus and reactive to the security measure, takes control of only the enterprise applications that employees are using.
MIM	Ensures document synchronization amongst multiple devices, primarily concern to data integrity and encryption, the access is applied by permissions and rules	Cannot deliver the client apps to the devices it will works with MDM or MAM to deliver the applications to mobile device, Limitation regards to access control and heavy focus and reactive to the security measure. Provide minimum protection against malware. MIM and MAM have similar limitations to MDM in regards to access control.
EMM	Capabilities to support the modern enterprise, as the focus shifts from devices to apps and content, Protect the digital assets and data of the firm, Respect and protect individual privacy, Drive adoption and provide visibility, assist in support and cost reduction, integrate with corporate identity, corporately enforce risk management control.	The complexity, Limited capability of the vast number of new mobile devices, very costly, require employee device compliance, the most capability of EMM is from MDM, needs expert to fill the gaps in the organization's skill set.
Desktop Virtualization model	Communicate via VPN connection, low cost because hardware costs can be more easily managed, centralize resources, reduce or eliminate to transmit data to the devices, reduce possibility of data	Needs expert, the admin needs to learn the VDI software's, server-side problems can affect multiple users everyone using that server or that image

	leakage, every user relying on that image benefits from the update.	
Access Control and Authentication	Ensure that the access is restricted, to authenticate each connection by organization before granting any access	Can be sniffed, if the access details obtained by unauthorized the person can access and gain all the permissions, relying only on the password, weak and simple password.
Remote Wiping	Helps to recover the device has be lost or stolen, wiped-provisioned device.	In some cases it can wipe the entire data private/corporate data, damage can happened before wiping, disconnected device from system or changing users/devices details can prevent wiping.
Dual Persona	Creating two environments on the same device, separate private apps and data from company's users can shift between two profiles without one affecting the other, same device can be used by two profile.	Needs huge save memory, the user can use the same password for both if the private password obtained malicious can also gain access to the corporate data.
NAC	Device cannot have access to the network before complying to the security policies, infected device with malware will be prevented to access, it rely on real-time so it will detect up normal behaviors, malware infections and other attacks are reduced or avoided	If the device is un-managed it cannot begin to the authentication server, we have three different BYOD topologies two of them can apply with unmanaged devices which NAC doesn't support it.

Table 3 The Pros and Cons of Different Technologies[34][75][30][36][48]

7.4 The Market Trends of BYOD

The number of mobile devices growing and employees demanding to use their own device increases [41], the organizations productivity increases as well because the staff continues to keep working on their own mobile devices whenever they can and at any time, even out of the office or at their time off from their work, ultimately BYOD increases the speed of the work which also increases the satisfaction of customers with fast response and good communication [65][70]. The main expectations are for increased personal productivity, flexibility of time and place and increased user satisfaction[76]. It's

clear that there are benefits for the organizations to improve their productivity, save work time, and cater to customer satisfaction as mentioned above These benefits will encourage companies and organizations to consider adapting BYOD on one hand and employee's demand of using their own device to work purpose on the other hand. This phenomenon will not benefit every kind of companies, according to Cisco and UNDP's interview they believe that BYOD will not be beneficial for industries because, as they explained, industries are using devices for the business purpose less, except the IT department and communication department, and Henrik from Cisco said, one industry with 500 workers will not pay for their subscriptions and take all the risks of BYOD for non-used device to the business, but maybe they will provide an Internet access for their workers as free services which can be covered without BYOD implementation (Cisco Interview). Cisco providing BYOD solutions to the companies and Henrik Stear said in the interview, the last five years have been the fastest growing market for Cisco's mobility of BYOD. Cisco and Apple have cooperating work based on integrating apple device into their enterprise for customer to collaborate telephone integration and video integration and stuff like that. The indications studies and research show that BYOD market is growing fast and it's gaining momentum with a strong trend today, particularly with Smartphone. BYOD is becoming more desirable for the enterprise, since it assists new trends in the workplace by connecting people all over the world [23]. The above-mentioned points are indication that the trend of adopting BYOD is increasing. Market researcher Gartner predicts that 85% of businesses from small and medium sized companies will have some kind of BYOD program in place by 2020 [77] [78] and it will become a normal policy for very businesses that employees bring their own device and they plug into the enterprise network [60] .

7.5 Economic Analysis

BYOD should not be a battle of wills between IT and employees, once organizations can see gains in employees productivity that BYOD offers, the companies should not rationalize it as a cost-saving method but they should look at it as a trend to reinvent potential work [42]. However, the device cost and flexibility cannot be the only factor to drive BYOD, most of the company's concern saving cost by adding part or fully device

purchasing on the employees. Even there are some up-front cost saving in BYOD like hardware and software per user [23] and service renting per user model, there is also operational cost and hidden cost which cannot be easy to predict or calculate without adopting a comprehensive BYOD first. A comprehensive BYOD is defined as; the organizations ability to monitor and wipe corporate data remotely, enforcing usage policies and corporate access automatically, dual persona of device configuration, device ability to move between networks seamlessly and securely, users ability to login by using multiple device, organizations corporate tools which collaborate with all end users devices, user-friendly, simple and authentication for all type of devices, and secure access through wired, WiFi, remote and mobile to the corporate network [42][46] [79]

the following figure illustrates comprehensive BYOD.

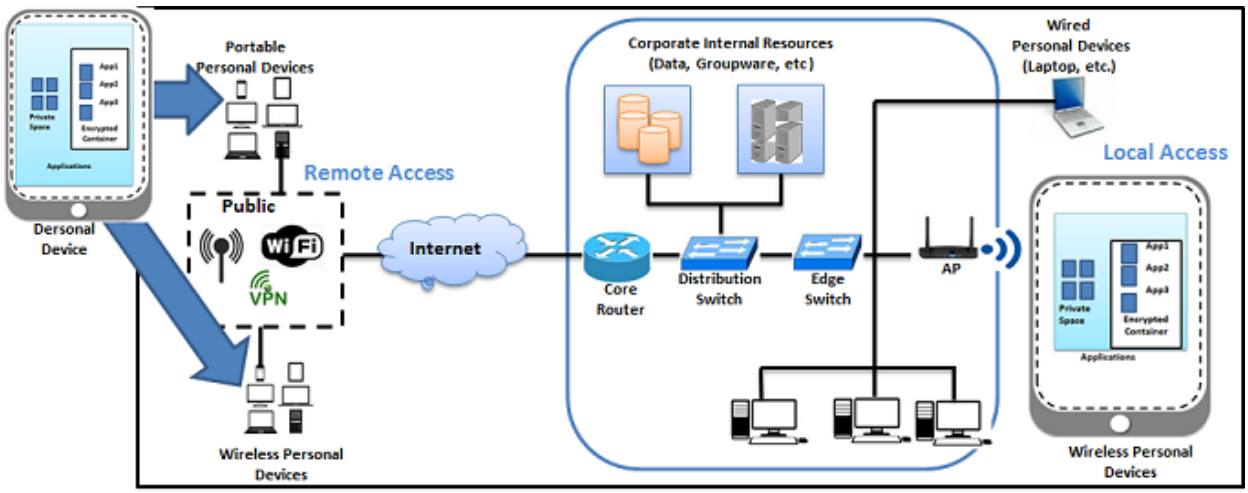


Figure 22 Diagram of BYOD and Smart-Work Environment [24]

This figure shows the diagram of BYOD and smart work environment and where the device can have access with any kind of access form and users' access by any type of mobile devices to the system, as well as systems control over the devices (interactive System or Comprehensive BYOD)

We can extract from the above figure that there are some saving cost elements such as the opportunity of creating a forum or other forms to support and that maybe the users are comfortable to work on WiFi access rather than cellular access which is helping organization to save purchasing data from tele company. On the other hand, there are a

lot of hidden cost, the operational cost is the major cost, for example, to build and implement the above architecture will also cost something for the company (technology and platform cost); to secure the connection and the network security will cost, this system will be built and function on the applications; the development of mobile applications will also be considered in the cost; help desk support and new mobile user will cost; and if the company provide a mobile cellular data within the country and abroad will add cost to the company's expenses because it is possible that the data would be used for users personal purpose. In the UNDP's interview Ognjen Krstulovic said, the organization will not save money by adopting BYOD, because they provide the same amount of money that supposed to use for buying mobile phone as company own device to the employee, but adopting BYOD mobile phone only is for employee's satisfaction and productivity. In another view, Moe Kyaw in UNDP Copenhagen said, they like BYOD just to get rid of asset management in the UNDP organization. Device defect and reparation is counted as a saving cost but at the same time Ogenjen in the interview said, for the mobile defect, there has agreement between the company and the provider for a subsidized repair for device defects in up to 2 years and for free but with the employees own device they cannot have such agreement with tele companies. Device recovery, mobile device integration, security safeguard is all part of the cost. Even though, there are some of those costs that will be there in the case of company owned device, most of them remains the same and adds more on BYOD adoption (Table 1 in chapter 3.5).The hidden costs can be the difficulty of managing different platforms, and BYOD solutions require the company to pay voice and data charges for their employees' devices [26]. Although, I don't have any statistical data related to the cost analysis about different technologies used for BYOD, but as a technology, the cost of virtualization solutions will be the cheapest mechanism because it is a centralized resource, and if we use the image created by IT Admins, each user will have a virtual portion. MDM and EMM are the costliest solution (Table 3 in sect 7.3) with the matter of vendor's payment and the complexity of solutions; it has a big role in the costs related to the operations and compliance. According to the information from Ognjen Krstulovic (UNDP interview) they can benefit from the idea of BYOD because they haven't used any device management control mechanism and they can use office365 which they have it already at work in the UNDP department to manage access

management and authentication mechanism and mobile devices remote wiping mechanism. On the other hand, Henrik Stear said, they are confident in adoption of BYOD by using MDM technology, so far he hasn't heard any security problems and he believed Cisco is earning money by adopting BYOD because Cisco pays only half price of the employee devices, and for employee's user guidance or any new information they have a forum to setup new information, but I haven't got any data evidence to confirm what he said (Cisco interview).

7.6 BYOD's Advantages and Disadvantage

There are some advantage and disadvantages for adopting BYOD; in the following table I will extract the advantages and disadvantages of BYOD. There may be more but I will focus on those in the security and economic perspective.

Advantages	Disadvantages
- The company will not be responsible to choose & buy a device to the employee - Company will not pay for most of software used by devices - Employees satisfaction, productivity, and flexibility - Customers satisfaction resulting of quick responding services - Having access to work anywhere at any time - Attract younger people, to make company modern and innovative - Creating balance between user's life and work - Stay the company competence	- Needs an extra platform and control management tools which is costs more - Companies data and confidentiality going to be under risks more - Needs strategy and policies which might be complicated - Its accessed remotely needs more data communication - There are lots of hidden cost which are not predicted - Needs more security tools - More challenges to the IT admin - Some security responsibility goes to the user

- The same device can be used for multipurpose	- Users privacy and confidentiality (device controlled by company)

Table 4The Advantages and Disadvantages of BYOD

7.7 Chapter Conclusion

In this chapter, the analysis was made based on the primary and secondary information collected from literature review, state-of-the-art and the interview with the companies. The chapter further presents the threat model, security analysis, market trend and the economy analysis of the BYOD. Despite some security issues, it was the increasing market trend of BYOD and the cost barrier that were also not seen as the major barrier for the BYOD deployment at this stage.

Chapter 8

8. Project Discussion/ Conclusion

8.1 Discussion

Even though, BYOD already exists today, it still remains as an informal practice for many organizations and only few of them formally adopted it. The reason of this is the lack of coherent approach to BYOD and the fear of companies being exposed to risks from security and compliance gaps to escalating IT complexity [7]. Organizations are already moving to design strategies to allow BYOD, employees who choose to get their best device will empower them to get their work done more efficiently and will have more satisfying work experience which will help organizations recruit and retain the best employees [7]. As well as in allowing bringing their own devices, it supports organizations' flexibility, mobility, and productivity. On the other hand, the contractors are increasingly required to use their own device rather than corporate equipment, that's why organization's practice for BYOD should be in their policies. The mentioned points encourage organizations, companies and enterprises to consider BYOD adaptation and proper BYOD policies. The willingness of employees to invest in BYOD is a major factor in the strong trend of BYOD phenomenon and it's growing steadily fast[41]. The costs that are associated with this phenomenon has multiple ways, some expecting to save cost while others expect the company will not lose the competition and gain, in results, from employees by new way of working employee, led innovation of job roles, and gain productivities. IEEE Consumer electronic magazines [26] wrote, sometimes the companies only look at the cost of the device, but when you look at the total picture, BYOD is more expensive, because of the fact that there are hidden costs and security risks. There are several risks associated in following BYOD such as, data leakage, applications vulnerability and network security, network availability, and device being compromise or lost. Having private and business data on the same device and using the same device as private and for work is risky; it might affect each other and one or both, personal or professional life may be compromise. The main challenge is different

dynamics of mobile adoption in different demographics, the way different people act when using devices. Magnified for companies that have large workforces spread across several geographic areas, and the IT department who is developing clear policies in advanced will be save from a lot of headache [60]. The other challenge is providing a bundle of devices especially with different OS, and integrate all devices into a consistent experience, the challenges for IT will be securing mobile devices, addressing app risks, and managing the mobile devices environment[80][37].

8.2 Conclusion

This research had a worthwhile contribution to BYOD and organizations, there are risks following BYOD and there are challenges to adopting it, from beginning when I start this research about BYOD with a simple knowledge about BYOD, I was made to believe that the risks are huge and cannot be solved, but after the research and literature review and with those interviews I have done from the people with experienced, I believe that there is a solution and it is manageable, MDM technology solved most of the risks. And in all three interviews, they confirm that the risks are manageable and they even confirm that a strong policy strategy would be a solution for most of the risks. The challenge for IT department is to adopt a correspondent strategy to the solution of their adapting BYOD. For example IT department of Cisco has implemented MDM to manage mobile devices in their BYOD adaption with key certification [Cisco Interview] their IT department found out this solution is reasonable and corresponds to their need with adopting BYOD.

About the economic impact, the need for consideration to collect data for BYOD cost analysis, it unfortunate to not be able to collect the practical data from the companies that's why I just focused on cost element analysis. I initially believed that the company can save costs by adopting BYOD but it turned out otherwise. The company will pay more to adopt BYOD compared to company owned device. However, company gains employee’s productivity and customer’s satisfaction and will stay competence to their competitions in the business market, which would be a great reason or opportunity of BYOD’s future sustainability and gaining market. I can say that, if the company is looking for saving cost by BYOD, this is not going to happen, but I will advise the companies if they want to stay competent and increase the employee’s productivity and benefit of

advance technology and modern mobile devices and customer's satisfaction they should embrace this phenomenon. So, IT department should optimize network security, management and performance to support mobile collaboration and BYOD strategies, support policy management, define related technology solution, simplify on-boarding for users, as well as for administrators offers proven expertise in networks, systems integration, and security practices [81].

8.3 Research Extension

This research can be extended by companies or BYOD vendor or anyone who would be interested to research more about economy impact and cost relation. Because of the matter of time consumption, I was not able to collect a practical data from companies to research about worth wise of cost relation to the BYOD.

References

References

[1] M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir, and E. H. M. Saad, “BYOD: Current state and security challenges,” *ISCAIE 2014 - 2014 IEEE Symp. Comput. Appl. Ind. Electron.*, pp. 189–192, 2015.

[2] “Enabling Seamless , Secure , and Mobile Experiences,” p. 707923, 2012.

[3] N. Selviandro, G. Wisudiawan, S. Puspitasari, and M. Adrian, “Preliminary study for determining bring your own device implementation framework based on organizational culture analysis enhanced by cloud management control,” *2015 3rd Int. Conf. Inf. Commun. Technol. ICoICT 2015*, pp. 113–118, 2015.

[4] S. Ali, M. N. Qureshi, and A. G. Abbasi, “Analysis of BYOD security frameworks,” *2015 Conf. Inf. Assur. Cyber Secur.*, pp. 56–61, Dec. 2015.

[5] Y. Kao and Y. Chang, “Managing Bring Your Own Device Services in Campus Wireless Networks.” 2015

[6] Z. Hallock, J. Johnston, F. Macias, R. Saville, and S. Tenneti, “Cisco Bring Your Own Device,” *Cisco*, no. 5, pp. 1–338, 2013.

[7] Citrix Systems Inc, “Best practices to make BYOD simple and secure,” pp. 1–10, 2012.

[8] Lily Chen, J. Franklin, and A. Regenscheid, “Guidelines on Hardware-Rooted Security in Mobile Devices (Draft),” vol. 164, no. SP 800-164, pp. 1–33, 2012.

[9] Cisco2014, “Cisco 2014 annual security report,” *Security*, pp. 1–81, 2014.

[10] S. Donaldson, S. Siegel, C. Williams, and A. Aslam, “Enterprise Cybersecurity,” *Apress*, pp. 119–129, 2015.

[11] M. Sagheb-tehrani, “Issues in Information Systems,” vol. 15, no. I, pp. 81–87, 2014.

[12] A. Services, “Bring your own device Agility through consistent delivery.”

[13] M. Mark, “A Brief History of BYOD and Why it Doesn’t Actually Exist Anymore,” 2013. [Online]. Available: http://raconteur.net/technology/success-with-enterprise-mobility. [Accessed: 10-Nov-2016].

[14] M. Souppaya and K. Scarfone, “NIST Special Publication 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise,” p. 30, 2013.

[15] “Publication Number : Title : Publication Date : NIST Special Publication (SP) 800-46 Rev . 2 Guide to Enterprise Telework , Remote Access , and Bring Your Own Device (BYOD) Security • Final Publication : http://dx.doi.org/10.6028/NIST.SP.800-46r2 (wh,” vol. 2, 2016.

[16] A. A. Morufu Olalere, Mohd Taufik Abdullah, Ramlan Mahmod, “Bring Your Own Device: Security Challenges and A theoretical Framework for Two-Factor Authentication,” vol. 4, no. 1, pp. 21–32, 2016.

[17] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students*. 2008.

[18] W. . Zikmund, J. . Babin, and M. Griffin, *Business Research Methods*. 2012.

[19] A. R. Ommani, “Strengths, weaknesses, opportunities and threats (SWOT) analysis for farming system businesses management: Case of wheat farmers of Shadervan District , Shoushtar Township, Iran,” *African J. Bus. Manag.*, vol. 5, no. 22, pp. 9448–9454, 2010.

[20] B. Phadermrod, R. M. Crowder, and G. B. Wills, “Developing SWOT Analysis from Customer Satisfaction Surveys,” *2014 IEEE 11th Int. Conf. E-bus. Eng.*, pp. 97–104, 2014.

[21] A. Sedigh, C. Campbell, and K. Radhakrishnan, “BYOT network solutions for

enterprise environment," *Proc. - UKSim-AMSS 16th Int. Conf. Comput. Model. Simulation, UKSim 2014*, pp. 489–493, 2014.

[22] A. Armando, G. Costa, "Changing user attitudes to security in bring your own device (BYOD) & the cloud," *Netw. Secur.*, vol. 2012, no. 3, pp. 5–8, 2012.

[23] V. Samaras, S. Daskapan, R. Ahmad, and S. K. Ray, "An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD," *11th Australas. Telecommun. Networks Appl. Conf.*, no. July, pp. 1–6, 2015.

[24] E. B. Koh, J. Oh, and C. Im, "A Study on Security Threats and Dynamic Access Control Technology for BYOD , Smart-work Environment," *Int. Multiconference Eng. Comput. Sci.*, vol. II, p. 6, 2014.

[25] K. W. Miller, I. Springfield, J. Voas, I. Fellow, G. F. Hurlburt, and C. Index, "BYOD : Security Considerations," pp. 53–56.

[26] Ogie, Robert, "Bring Your Own Device : Bring & Your & Own & Device :," *Us-Cert*, no. February, pp. 78–81, 2013.

[27] M. Mark, "Success with enterprise mobility - raconteur.net," 2013. [Online]. Available: http://raconteur.net/technology/success-with-enterprise-mobility. [Accessed: 10-Nov-2016].

[29] I. Forrester Research, "Key Strategies To Capture And Measure The Value Of Consumerization Of IT Enterprises Achieve A Wide Range Of Benefits By Deploying Bring-Your-Own-Device Programs," *Trend Micro*, no. May, pp. 1–17, 2012.

[30] ADoD Intelligence and Security, "Risk Management of Enterprise Mobility Including Bring Your Own Device," 2013. [Online]. Available: http://www.asd.gov.au/publications/csocprotect/enterprise_mobility_bring_your_own_device_byod.htm.

[31] R. C. Basole, "Enterprise mobility: Researching a new paradigm," *Inf. Knowl.*

Syst. Manag., vol. 7, pp. 1–7, 2008.

[32] B. Morrow, “BYOD security challenges: Control and protect your most sensitive data,” *Netw. Secur.*, vol. 2012, no. 12, pp. 5–8, 2012.

[33] Y. Wang, J. Wei, and K. Vangury, “Bring your own device security issues and challenges,” *2014 IEEE 11th Consum. Commun. Netw. Conf.*, pp. 80–85, 2014.

[34] K. Downer and M. Bhattacharya, “BYOD Security : A New Business Challenge,” *5th Int. Symp. Cloud Serv. Comput. (SC2 2015)*, pp. 1128–1133, 2016.

[35] M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir, E. Hisham, and M. Saad, “BYOD : Current State and Security Challenges BYOD : Current State and Security Challenges,” no. August 2015, pp. 189–192, 2014.

[36] J. Viega and B. Michael, “Mobile Device Security,” *IEEE Secur. Priv. Mag.*, vol. 8, no. 2, pp. 99–101, 2010.

[37] EY, “Security and risk considerations for your mobile device program,” *Insights governance, risk compliance*, no. September, p. 12, 2013.

[38] T. A. Yang, R. Vlas, A. Yang, and C. Vlas, “Risk management in the era of BYOD the quintet of technology adoption, controls, liabilities, user perception, and user behavior,” *Proc. - Soc. 2013*, pp. 411–416, 2013.

[39] A. Scarfo, “New security perspectives around BYOD,” in *Proceedings - 2012 7th International Conference on Broadband, Wireless Computing, Communication and Applications, BWCCA 2012*, 2012, pp. 446–451.

[40] J. M. Chang, “Securing BYOD,” pp. 9–11, 2012.

[41] J. Loucks, R. Medcalf, L. Buckalew, and F. Faria, “Horizons The Financial Impact of BYOD Top 10 Global Insights from the Cisco IBSG Horizons Study,” *Cisco*, pp. 1–6, 2013.

[42] CISCO IBSG Horizons, “The Financial Impact of BYOD A Model of BYOD’s Benefits to Global Companies,” *CISCO IBSG Horizons*, pp. 1–26, 2013.

[43] K. Findings, “Cool Vendors in Cloud Security Services , 2011,” no. April, 2011.

[44] T. Kim and H. Kim, “A system for detection of abnormal behavior in BYOD based on web usage patterns,” *2015 Int. Conf. Inf. Commun. Technol. Converg.*, pp. 1288–1293, 2015.

[45] S. G. Ocano, B. Ramamurthy, and Y. Wang, “Remote mobile screen (RMS): An approach for secure BYOD environments,” *2015 Int. Conf. Comput. Netw. Commun. ICNC 2015*, pp. 52–56, 2015.

[46] “https://www.whatech.com/enterprise-software/250-mobile-device-management/14890-big-benefits- by-being-strategic-about-byod,” p. 14890.

[47] K. Rhee, W. Jeon, and D. Won, “Security requirements of a mobile device management system,” *Int. J. Secur. its Appl.*, vol. 6, no. 2, pp. 353–358, 2012.

[48] M. Souppaya and K. Scarfone, “User’s Guide to Telework and Bring Your own Device (BYOD) security,” *NIST Spec. Publ. 800-114*, 2016.

[49] E. G. Mobile, “When is Enough Mobile Security Actually Enough ?,” no. April, 2013.

[50] N. Leavitt, “Today’s mobile security requires a new approach,” *Computer (Long. Beach. Calif).*, vol. 46, no. 11, pp. 16–19, 2013.

[51] R. Review, “Q4 Mobile Security and Risk Review,” pp. 1–13, 2016.

[52] “Why mdm needs standalone mam,” p. 8740.

[53] M. Hasson, “Mobile Application,” *Techopedia*, 2013.

[54] K. Scarfone and P. Hoffman, “Guide to Security for Full Virtualization Technologies Recommendations of the National Institute of Standards and Technology,” *Natl. Inst. Stand. Technol. Spec. Publ.*, no. 800–125, pp. 1–35, 2010.

[55] M. A. Delivery and T. N. Frontier, “1 2 3 4.”

[56] S. Butler, “Must-Have Capabilities to Optimise Enterprise Mobility,” pp. 1–7, 2014.

[57] M. Toft, “Securing the modern Enterprise !”

[58] Jack Madden, “In 2016, many of the tools and concepts for enterprise mobility are ready to go.” .

[59] Gartner, “Login Page,” 2015. [Online]. Available: http://www.gartner.com/document/code/252621?ref=ggrec&refval=2953219. [Accessed: 10-Nov-2016].

[60] Y. O. U. Asked, “What’s the,” pp. 1–9, 2014.

[61] G. Costantino, F. Martinelli, A. Saracino, and D. Sgandurra, “Towards enforcing on-the-fly policies in BYOD environments,” *2013 9th Int. Conf. Inf. Assur. Secur. IAS 2013*, pp. 61–65, 2014.

[62] R. Balebako, A. Marsh, J. Lin, J. Hong, and L. Cranor, “The Privacy and Security Behaviors of Smartphone App Developers,” *Internet Soc.*, no. October, 2014.

[63] I. C. Technologies, “Todays Lecture • Part II : A New Enterprise Cybersecurity Architecture,” vol. 3, no. Icte 3, 2015.

[64] M. La Polla, F. Martinelli, and D. Sgandurra, “A Survey on Security for Mobile Devices,” *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 446–471, 2013.

[65] G. Costantino, F. Martinelli, A. Saracino, and D. Sgandurra, “Towards Enforcing On-The-Fly Policies in BYOD Environments 20J 39th International Conference on Information Assurance and Security (IAS),” pp. 61–65, 2013.

[66] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, 800-61. Revision 2,” *NIST Spec. Publ.*, vol. 800–61, p. 79, 2012.

[67] P. Kotler, “Marketing Management, International Edition.” 2003.

[68] G. J. Hay and G. Castilla, “Object-Based Image Analysis: Strengths,

Weaknesses, Opportunities and Threats (SWOT)," *OBIA, 2006 Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.*, p. 3, 2006.

[69] O. Human and S. Behavior, "Strengths and Weaknesses." .

[70] K. AlHarthy and W. Shawkat, "Implement network security control solutions in BYOD environment," *Proc. - 2013 IEEE Int. Conf. Control Syst. Comput. Eng. ICCSCE 2013*, pp. 7–11, 2013.

[71] N. Burns-sardone, "Making the Case for BYOD Instruction in Teacher Education," *Issues Informing Sci. Inf. Technol.*, vol. 11, pp. 191–201, 2014.

[72] I. UNDP, "Frequently Asked Questions | UNDP." [Online]. Available: http://www.undp.org/content/undp/en/home/operations/about_us/frequently_askedquestions.html#being. [Accessed: 10-Nov-2016].

[73] Jessica Keyes, "BYOD: Mobile Devices Threats and Vulnerabilities." [Online]. Available: http://www.ittoday.info/ITPerformanceImprovement/Articles/2014-07Keyes2.html.

[74] Y. J. Ham, H.-W. Lee, J. D. Lim, and J. N. Kim, "DroidVulMon -- Android Based Mobile Device Vulnerability Analysis and Monitoring System," *2013 Seventh Int. Conf. Next Gener. Mob. Apps, Serv. Technol.*, pp. 26–31, 2013.

[75] S. Insight, "Enterprise Mobility Management 2012 : the Global Perspective," no. June, 2012.

[76] M. Brodin, J. Rose, and R.-M. Åhlfeldt, "Management Issues for Bring Your Own Device," *Eur. Mediterr. Middle East. Conf. Inf. Syst. 2015*, vol. 2015, pp. 1–2, 2015.

[77] "BYOD/BYOA: A Growing, Applicable Trend | Inc.com," 2016. [Online]. Available: http://www.inc.com/comcast/byod-byoa-a-growing-applicable-trend.html. [Accessed: 10-Nov-2016].

[78] B. Giorgio, "What Is BYOD ? Challenges and Opportunities." [Online]. Available:

http://blog.parallels.com/2014/12/10/what-is-byod/. [Accessed: 10-Nov-2016].

[79] “Big benefits by being strategic about BYOD - WhaTech,” 2013. [Online]. Available: https://www.whatech.com/enterprise-software/250-mobile-device-management/14890-big-benefits-by-being-strategic-about-byod. [Accessed: 10-Nov-2016].

[80] F. Report, “Trends in enterprise mobility,” no. April, 2013.

[81] D. The, “Readying the network for mobile collaboration and BYOD.”

[82] Z. Zhao and F. C. Colon Osono, “‘TrustDroid???’: Preventing the use of SmartPhones for information leaking in corporate networks through the used of static analysis taint tracking,” *Proc. 2012 7th Int. Conf. Malicious Unwanted Software, Malware 2012*, no. March 1999, pp. 135–143, 2012.

[83] K. Alharthy, “Implement Network Security C ontrol S olutions in BYOD Environment,” pp. 7–11, 2013.

[84] Cisco, “2013 Cisco Annual Security Report,” pp. 1–41, 2013.

[85] H. D. Dowxu, N. Hwi, X. Ed, Y. G. Dowxu, D. Hgx, F. Wrrov, D. Q. G. Whfkqltxhv, and X. E. Dwwdfnhuv, “([Sorlwdwlrq.”

[86] R. Absalom, “On the Radar : Apperian MAM Mobile application management and enterprise app store,” no. May, 2015.

[87] B. Title, “Bring Your Own Device (BYOD) and Security Configuration,” pp. 1–4.

[88] M. Lock, “RUNNING LEAN ANALYTICS WITH A CLOUD,” no. April, 2016.

[89] “Perceptual-Control-Based Model Mobile Information Management Ni Wang*, QingYi Hua, YaMing Li, Cui Guo, XiaoDong Qi,” pp. 421–424, 2011.

[90] E. Look and F. Range, “MAM + MDM : ENTERPRISE MOBILITY AT SCALE MAM : MDM CUSTOMER USE CASES cont . Healthcare and Insurance Provider MAM : MDM.”

[91] D. R. Tobergte and S. Curtis, “No Title No Title,” *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2013.

[92] N. Fani, R. V. O. N. Solms, and M. Gerber, “Governing Information Security Within the Context of ‘ Bring Your Own Device in SMMEs ,’” pp. 1–11, 2016.

[93] B. Tokuyoshi, “The security implications of BYOD,” *Netw. Secur.*, vol. 2013, no. 4, pp. 12–13, 2013.

[94] F. Li, C. T. Huang, J. Huang, and W. Peng, “Feedback-based smartphone strategic sampling for BYOD security,” *Proc. - Int. Conf. Comput. Commun. Networks, ICCCN*, no. Section III, 2014.

[95] National Instruments, “Understanding the Total Cost of Embedded Design,” pp. 1–10, 2012.

[96] A. Insight, “Servicing Enterprise Mobile Apps : The ITSM Difference,” 2013.

[97] D. Gessner, J. Girao, G. Karame, and W. Li, “Towards a user-friendly security-enhancing BYOD solution,” *NEC Tech. J.*, vol. 7, no. 3, pp. 113–116, 2013.

[98] CISCO, “BYOD Security Challenges in Education: Protect the Network, Information, and Students BYOD Security Challenges in Education,” 2012.

[99] A. Mishra and K. Jani, “Comparative study on bring your own technology [BYOT]: Applications & security,” *Int. Conf. Electr. Electron. Signals, Commun. Optim. EESCO 2015*, 2015.

[100] W. Paper, “Avoiding BYO Policy and Security Pitfalls,” *Citrix*, 2014.

[101] S. Owens, “The Total Economic Impact™ Of Cisco Identity Services Engine - Cost Savings And Business Benefits,” no. October 2013, pp. 1–21, 2013.

[102] L. I. N. Defence and S. Innovation, “Leaders in.”

[103] J. Rapoza, “9699-CUR-MA-BYOD-Increasing-costs-JR,” 2014.

[104] R. Absalom, “International Data Privacy Legislation Review: A Guide for BYOD

Policies," *Ovum*, no. May, pp. 1–23, 2012.

[105] P. Bruder, "GADGETS GO TO SCHOOL: The Benefits and Risks of BYOD (Bring Your Own Device).," *Educ. Dig.*, vol. 80, no. 3, pp. 15–18, 2014.

[106] S. Butler, "Enterprise Mobility Management: Changing it Up with CYOD," 2014.

[107] J. Seigneur, P. Kölndorfer, M. Busch, and C. Hochleitner, "A survey of trust and risk metrics for a byod mobile working world," *Third Int. Conf. Soc. Eco-Informatics*, pp. 11–22, 2013.

[108] B. Hoffman, "WHITE PAPER CYOD : The End of BYOD as We Know It ?," no. June, 2014.

[109] S. Bass, "Security Within Desktop Virtualization."

[110] W. Peng, F. Li, K. J. Han, X. Zou, and J. Wu, "T-dominance: Prioritized defense deployment for BYOD security," *2013 IEEE Conf. Commun. Netw. Secur. CNS 2013*, pp. 37–45, 2013.

[111] F. Employees and M. D. Challenges, "Solutions for Secure Mobile Devices," 2014.

[112] N. Castellina, "Mobile Erp: Taking Erp Roi Into Your Own Hands," 2014.

[113] Aruba, "The Definitive Guide to BYOD," *Aruba Corp.*, p. 60, 2013.

[114] G. L. Boon, "A Review on Understanding of BYOD Issues , Frameworks and Policies," *3rd Natl. Grad. Conf. (NatGrad2015), Univ. Tenaga Nas.*, no. April 2015, pp. 8–9, 2016.

[115] G. State and O. F. Enterprise, "Global State of Enterprise Mobility 2016," p. 23, 2016.

[116] "Taking an architectural approach to BYOD."

[117] B. Omg, B. M. Gaff, and M. Will, "Computing and the law.," *Health Serv. J.*, vol. 103, p. suppl 1-8, 1993.

[118] I. Average, “Mastering MALM : The Enterprise Mobile Application Lifecycle,” 2013.

[119] A. Armando, G. Costa, and A. Merlo, “Bring your own device, securely,” *Proc. 28th Annu. ACM Symp. Appl. Comput. - SAC ’13*, p. 1852, 2013.

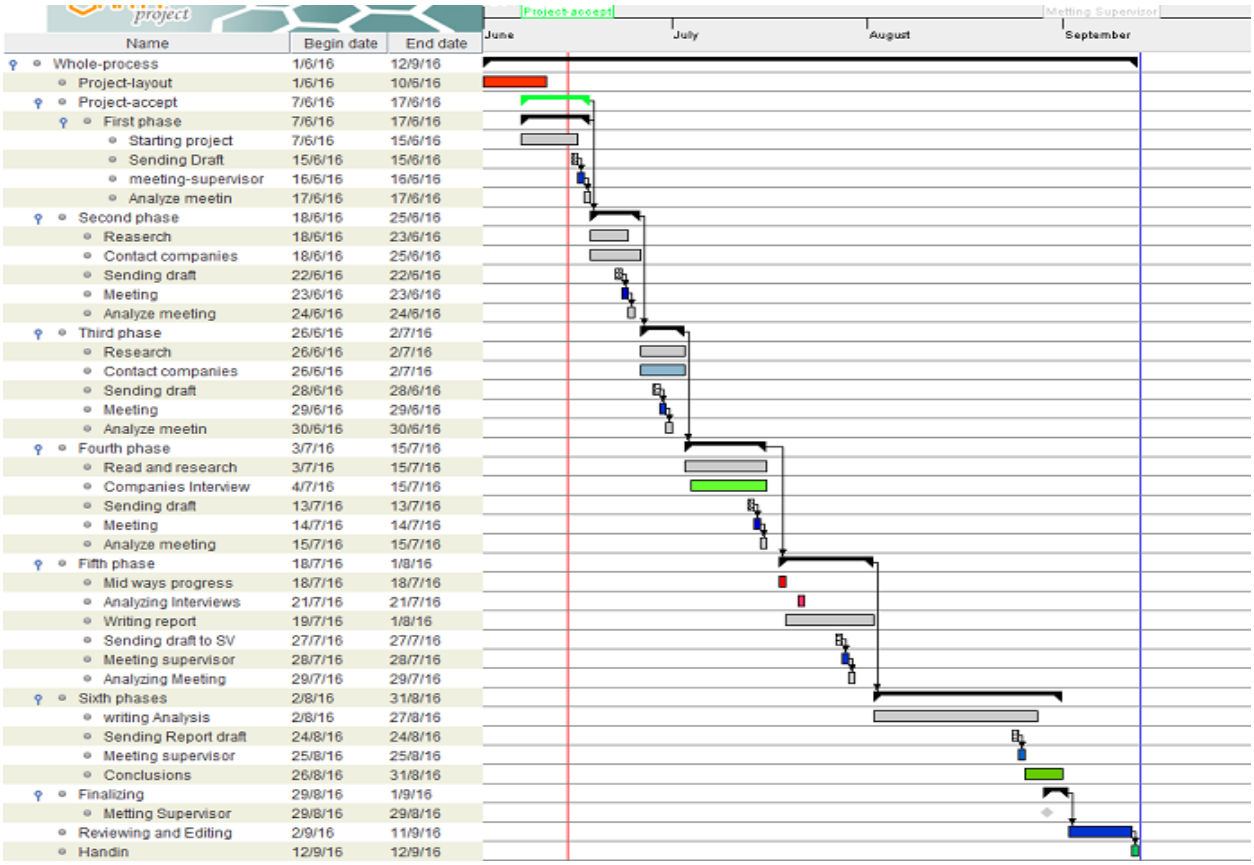
[120] H. Olesen and S. Khajuria, “Fine - grained control of user attributes : T he case of Bring Your Own Device (BYOD).”

Appendix

Appendix

Appendix 1: Project Gantt chart

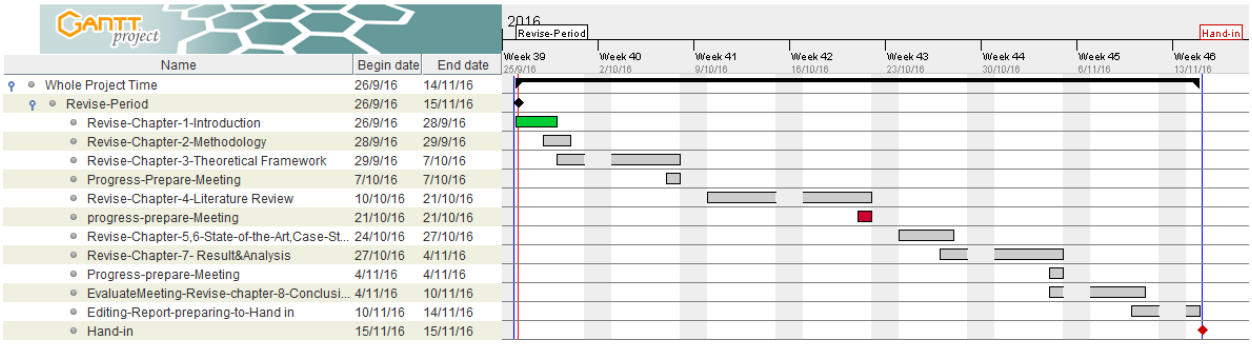
The Figure is Time frame project management by using Gantt chart.



Name	Begin date	End date
Whole-process	1/6/16	12/9/16
Project-layout	1/6/16	10/6/16
Project-accept	7/6/16	17/6/16
First phase	7/6/16	17/6/16
Starting project	7/6/16	15/6/16
Sending Draft	15/6/16	15/6/16
meeting-supervisor	16/6/16	16/6/16
Analyze meetin	17/6/16	17/6/16
Second phase	18/6/16	25/6/16
Reaserch	18/6/16	23/6/16
Contact companies	18/6/16	25/6/16
Sending draft	22/6/16	22/6/16
Meeting	23/6/16	23/6/16
Analyze meeting	24/6/16	24/6/16
Third phase	26/6/16	2/7/16
Research	26/6/16	2/7/16
Contact companies	26/6/16	2/7/16
Sending draft	28/6/16	28/6/16
Meeting	29/6/16	29/6/16
Analyze meetin	30/6/16	30/6/16
Fourth phase	3/7/16	15/7/16
Read and research	3/7/16	15/7/16
Companies Interview	4/7/16	15/7/16
Sending draft	13/7/16	13/7/16
Meeting	14/7/16	14/7/16
Analyze meeting	15/7/16	15/7/16
Fifth phase	18/7/16	1/8/16
Mid ways progress	18/7/16	18/7/16
Analyzing Interviews	21/7/16	21/7/16
Writing report	19/7/16	1/8/16
Sending draft to SV	27/7/16	27/7/16
Meeting supervisor	28/7/16	28/7/16
Analyzing Meeting	29/7/16	29/7/16
Sixth phases	2/8/16	31/8/16
writing Analysis	2/8/16	27/8/16
Sending Report draft	24/8/16	24/8/16
Meeting supervisor	25/8/16	25/8/16
Conclusions	26/8/16	31/8/16
Finalizing	29/8/16	1/9/16
Metting Supervisor	29/8/16	29/8/16
Reviewing and Editing	2/9/16	11/9/16
Handin	12/9/16	12/9/16

Revise Gantt chart

The Figure is Time frame of Revise project by using Gantt chart



Name	Begin date	End date
Whole Project Time	26/9/16	14/11/16
Revise-Period	26/9/16	15/11/16
Revise-Chapter-1-Introduction	26/9/16	28/9/16
Revise-Chapter-2-Methodology	28/9/16	29/9/16
Revise-Chapter-3-Theoretical Framework	29/9/16	7/10/16
Progress-Prepare-Meeting	7/10/16	7/10/16
Revise-Chapter-4-Literature Review	10/10/16	21/10/16
progress-prepare-Meeting	21/10/16	21/10/16
Revise-Chapter-5,6-State-of-the-Art,Case-St...	24/10/16	27/10/16
Revise-Chapter-7- Result&Analysis	27/10/16	4/11/16
Progress-prepare-Meeting	4/11/16	4/11/16
EvaluateMeeting-Revise-chapter-8-Conclusi...	4/11/16	10/11/16
Editing-Report-preparing-to-Hand in	10/11/16	14/11/16
Hand-in	15/11/16	15/11/16

Appendix 2: Cisco Interview

The questions asked at Cisco interview:

1- Your name and your job position in Cisco?
2- How long you are working with Cisco?
3- What is BYOD in Cisco's definition?
4- Why BYOD? I mean why do we need BYOD?
5- What part of BYOD Cisco dealing with at most? In part I mean with Business part, IT, Economy part, HR, Legal, Employee, Technical part, Security part …
6- Since when Cisco started to be concern about BYOD solution?
7- Is Cisco using BYOD itself for workers?
8- What kind of risks Cisco experienced with BUOD?
9- If we level the security of BYOD from 1-5 what level it is secure?
10- How many types of risks are covered until now?
11- Before we go to the 11areas of enterprise security, what is BYOD risk assessment for Cisco?
12- Which of the risk is most difficult to solve?
13- What does these terms mean for Cisco MDM, MAM, MIM, and EMM?
14- How difficult is to control security for multifactor device and multi operating system?
15- Don't you thing that the data traffic will be another issue in the future of all those devices connection and communication?

16- What does the employee have to do to assist more security on BYOD?
17- What are the biggest challenges of BYOD security that Cisco will strongly be consider? We can have this question again for the 11 areas of enterprise.
18- Confidentiality, Integrity, Availability are three concern parts of enterprise and businesses, which one will be most in risk by using BYOD?
19- What is Cisco's experience or information about compromising system or system attach happened by using BYOD?
20- What are BYOD risks? (Access, Confidentiality, Complexity, Malware, Legal and Regulatory, Bandwidth, Breach, Data Storage)

Mobile and BYOD are additional enterprise endpoints, which are not owned or managed by the organization. Enterprises need to plan for the protection of these devices as an integral part of their overall endpoint, server, and security functional area strategy for this rezones Enterprise security has 11 functional areas can we go through of them to see which one is really related and have to do something about it for BYOD security?

1- System Administration (Multifactor authentications)
2- Network security (Firewall)
3- Application Security (MAM)
4- Endpoint, server, and device security (MDM)
5- Identity, Authentication, and access management (Strong Authentications)
6- Data protection and cryptography
7- Monitoring, Vulnerability, and patch management
8- High Availability, Disaster Recovery, and Physical protection
9- Incident response
10- Asset Management and Supply Chain
11- Policy, Audit, E-Discovery, and Training

Some Business questions…

21- What are the key market trends of BYOD? (this is a little business side question)

22- Some researcher says company saves money by BYOD and some other saying no it costs more, what is your opinion?
23- What are the market opportunities and threats faced by the key vendors (Cisco for example)?
24- What are the strengths and weaknesses of the key vendors (Cisco for example)?
25- What will the market size be in 2018 and what will the growth rate be?

Appendix 3: Cisco Interview Transcription

Cisco Interview Transcription

Date of interview, 08/07/2016 time- 12:30 til 14:00 ate Cisco department Cisco Lautrupsgade 7, CPH Nordhavnen

CISCO **Henrik Staer** | **Manager Systems Engineering** | Cisco Denmark | hstaer@cisco.com | Mobile: +45 40205511| Single No# +45 39585034

My name is ahmad, i have master thesis in alborg uni which is dealing with security risks associated with byod, lately byod lately byod became popular and there are a lot of situations with the security so i want to research about that and expand my thesis with this subject.

2:45 Per Jensen, consulting system Engineer, working 22 years in Cisco, Henrik stear SE manager in Cisco 17 years in Cisco.

q1, whay is the definition of byod by cisco? the definition of Cisco for byod? 3:28 the definition is we targeting enterprise customers and bring your device we defined as the possibility for the employees of cretan organization to bring their own device to carry their own mobile device phone, tablet or what have any kind of and get more access to company resources than normally you just get internet access.

me, basically the definition is like the general one.

5:22 me, why do we have BYOD now? Because enterprise had their own device and work properly?

we have it because of the change in work life balance, we have it because it is possible, we have the devices as a private person which it has a power it has the possibility to be used as your working device, so now we have the integrations we have a lot of stuff running as a private person on your iphone or your android and the same device is powerful enough to own and carry your business applications. So with the integration of your work life and your private life you get the integration that it is an advantage for the company and for the employee that you mix that on one working device. so we have our devices as we have all our applications as we can have all our applications on our own, this is my device but i use it as my working device as well. i have all my company applications i can have on this device.

6:58 so you can be at your daughters hand ball game and kind of proof something for your internal system because you bring your own device so instate of you drive back to the office or whatever to get or do it when he is watching football game. so the driver is because we can because the technology is here, the devices are strong enough and because we need it for work life balance perspective. the bounder is on the you know when i started to work i get in the office the day and i left at 4 pm, and when i exit the office there is nothing i can do. today this is totally gray area I don't really know when i am, when do i stop work, because i always have the option just to check, i have my private email i have my working exchange email on this device, I can at any time when I am watching my daughters football when I am at party I bring my device under the table just to check is anything important going on, so if anything important going on its easier for me as person to deal with that possibly to get other people to go on, or possibly to say yes or no, or to say don't do that stop that and so on immediately, I do that 9 clock in the evening or 7 in the morning. so I think the two drivers because we can because of the technology and because of the need to change the way we work. if the business need was not their i don't thing just the powerful device wouldn't do the trick. its really need, it the human nation need to be online and to be able to do things much more flexible and we did when I started work.

Me, but the company providing device to do thesis things was not enough? No because it was only for work, when this device was purely owned and control by IT department of company I was not even able to watch a webpage privately and I want to only one device carry it with me. So you have one device which everything is possible. When I was working with TDC I had their laptop I could do nothing at all with laptop it was lock it, if I even want to upgrade I couldn't do it. so (flexibility, productivity and multipurpose) is BYOD.

11:05 before when we didn't have BYOD I was under control of IT department and i was under control what was test it in the IT department and what the IT department wanted me to know but now it’s totally free.

Me, so after those benefit of BYOD everybody is not professional of using devices some issue of security will pop up. the question is those benefits of BYOD worth it of bring a lot of security risks to the company? yes there is security risks but IT department has BYOD security policy I have certificate on my private device if anything happened or I lost my device the IT department will wiped. I have agreed to terms that if something happened even my private pictures will be wiped. IT department need to have a policy to mobile device management, and the user need to agreed.

Q, what part of BYOD Cisco is really dealing with for the business? we are highly dealing with security. We have software and hardware for that, the infrastructure is significant part of Cisco business. Policy server controls access to the network and integrated with MDM system.

16:29 Q, if one employee is not agree to this policy is their another policy or agreement for the manage device? you can always have internet access but we have all one device policy for all its in or out.

16:52 Q, when Cisco start to use BYOD, answer 5 years ago, in different forms because it has developed. First time i saw a real BYOD policy where i could understand what i allowed to do, we have a parameter policy (what are you allowed to do when you are mobile user, and connected user when you are wifi user so there is good description, i thing its 4 years ago).

17:43 Q, what kind of risks Cisco experienced with byod until now? if there were any we would not know, our IT department will see it but not tell us(we don't know its happened or no, I haven't seen any case which we have been compromised due to the byod policy).

19:00 Q, the level of byod security device from one to five grade what level would be in Cisco? I thing security can always be better and risk never be zero that's why i give 4.

I thing its trade-off if you have really really tide security it would not be flexible. I thing its good and work for our life we have no issues.

20:10 what do you know about the 11 functional area of enterprise? we haven't hear about that. maybe our IT department potentially have information about that. but what I know is we have different policies based on the time as, where you are in the promises or out are byod or company owned and so on.(different policies for different devices)

6 character access control on the device policy we have.

26:45 Q, MDM, MAM, MIM, EMM, are 4 terms what do you know about those? when we use byod solution we are typically always integrate to a third party MDM.

27:37 Q, how difficult is to control security in multifaceted device and operating system? Like Android, IPhone windows and so on. its difficult of challenging but you have a variety of OP, we have an opportunity to register our device from our policy server we will push a sign certificate to the device, so that not every time have to to the same process, just work by connecting it. when we try the registration the device connect to the registration port so that displays a kind of registration page on my screen, the I am using my active directory and my password, if that is successful i get the opportunity to register my device and that means from our policy server will push certificate to the device so that will be located on the device next time when i connect it will recognize my device. so this registration has worked different for different devices and that's the case.

we support only Apple and Android device I don't know about windows if we do. but the different variety of device the more level of OS the more different it behave but today at least for android and apple it works pretty seamless.

31:51 Q, don't you think it will be a data traffic problem in the future by using byod and IoT all depends on Internet connection?

i don't think it gonna be difficult because it going to be in the other scale, I can have different devices registered if I lost my device i can login to my profile in the self-service portal and tell this device is loss it the it will be wiped then it will inform the policy server and policy server will inform MDM system for wiped and it will give different access to connected anyway it's all automatic but IT department has to get to this work get all the connections. The problem is if the user doesn't deploy the additional security and addition policy the n we getting really problem.

The challenges for IT would be if the company do not deploy addition security, in the future it's gonna be multimillion devices connected not device itself but if it's not gonna deploy addition security and addition policy of how you want to handle this, that's the challenge.

37:04 Q, what does the employee has to do to assist the more security on byod?

Follow the rules apply to the roles, and do not visit strange sites do not click on strange links and have a good IT behavior.

Q, but so what the company should do to employee follow those roles? we do get educate them to have a good behavior on the internet, and we do educate about our IT policies how do we act as employees security wise. for example, we are allowed to use face book but we do educated about what not to do on face book.

we do have some suspicious links if you visit we will get a call from our internal IT and will says you have just bridge the security policy don't do that, there is no penalty for that.

so the answer of the question is educate people and in real life give people little warning it was a face email send by and you click it but do not click those things.

42:48 what are the biggest challenge of byod security that Cisco will strongly be consider?

the biggest challenge in the market is awareness, first is 2 things for that first is the company invest enough in security that they take it seriously, and second is the awareness how the people behave on the internet with IT, the first one is extremely important the company they cut the budget when they need to invest in the security. Some of the threats they face they can close the company.

you can say the describe of security discussion we would like to take with the customer is we call it before during and after,(the before is the protection , during the mean is some company is compromised but they don't know it takes time till they find out that they compromised, and after is what they will do when they found out that they compromised).

46:37 Q, what is the most byod security risks is risky for the company? The bridges is biggest risk, and the things we don't know is most risky, the creativity of internet criminals are most risky because we don't know what they gonna do and how they hit us.

for the authentications they have factor authentication.

for the protection they use firewall and intrusion detection system with anti-malware system.

50:33Q, what do you know about your data protection and cryptography? they don't know but they don't thing that the uses this mechanism.

about the disaster recovery the IT department will wipe the device and will register when the employee use a new device.

51:49 they bring their own device and the fully access and control permeated to Cisco it department to manage the device, and Cisco paying for the subscription its half half. supply chain is android and apple, they have two models on Cisco if you want an apple

device we get supplementary cost coverage, we pay part of it ourselves if you get lower grade price it covered by Cisco.

55:08 what will be the market size of byod used by company in 2018? now it's about 10%

we thing it will be about 23-23% .

byod is not so much used now because they don't have a strategy for it, and they don't have a policy base access in place, otherwise security and economy is not a problem. BYOD is well known but they don't know yet what they will do about it and they don't have a strategy.

the directors in the company they says we want BYOD but they don't know how and why. and before you have to have BYOD you have to have some infrastructures ready in place62:47 .

The policy based control of the infrastructure that's where they are today, so before that you gave to have a policy and its a big project they have a thousand of access need to fixed. and this is highly related to security.

67:26 Q, why do you thing Cisco implementing BYOD, is it for flexibility or save money or what is the main reason? the purpose is the driver and attracting younger people, to make Cisco modern and innovative company's work form, to create the best work space for employees then of-course flexibility and calling cost, increase productivity comfort ability, and people work more things are moving faster much faster. and for international company like Cisco different time zone, we have people working in different working time zone, it's like we work whole days because of time zones, sometimes we respond when some other sleeping and they respond when we are sleeping. (Productivity, flexibility, and attracting place work with flexible work life balance these are key point of using byod).

71:05 someone says by implementing BYOD Company saving money and some others says they lose money. Potentially BYOD is not for everyone, if you have a manufacturing company, you may have administration but you have a huge number of

manufacturing people which they may not have bring your own device. So BYOD is for the company that they really need BYOD, because if you if you give sim-card to everyone it may be a huge impact to the cost, its basically a pure HR policy. example people in the factory will not get it and people in the administration in certain level will get it.

74:55 Q, what are the market opportunities for BYOD, the market opportunity is massive, we have education systems which is massive opportunity for Cisco to sell infrastructure and security systems. the last 5 years is one of the fastest growing markets for the Cisco mobility of BYOD, Cisco and Apple have working relationship based on integrating apple devices into our enterprise customers that's from all point of view make easier for bring your own device to collaboration telephone integration and video integration and stuffs like that Q, how about threats? Threat is also opportunity because threats Demand Company like Cisco develop protection systems against the threats. So that's opportunity, so the more and the more advanced the criminals on the internet become the more companies need to invest in the security system. But its clear that when more and more of these devices are connected and have access to the company's resources the threat and malware will increase.

77:18 Q, what are the strength point and weakness? Flexibility, which is always connected, and we respond to the people when they need it, we stay always connected and the whole society remains connected. and the weakness is you are always on and threats, discipline, education will be weakness because its moving so fast and its difficult to make people educate fast enough so that they know how to behave how to understand threats how to do it and what to do.

the companies are using peoples lack of knowledge so the education is a clear threat.

81:01 last Q, what do you thing would be the market size of BYOD in the near future let’s say 2018, in Denmark it will grow slowly it will nearly 20-25% maybe 30% in the near to 2-3 years, you need to write in your report company have to invest more in security and BYOD, because they don't invest on it they just expected to get it for free, and when they get to the table they are going to buy it they see what is cost then they

will say we will use this for something else it may not hit they hit people over there. That's what they do because they are all cost constrained. So the investing on security will be the best option of the company.

82:44 thank you so much for your time and you corporations.

82:47 you welcome, not problem

Appendix 4: UNDP Bosnia-Herzegovina Interview Transcription

Questions:

1. What is your name &what is your job position in UNDP?
2. How long you are working with UNDP?
3. What is BYOD in your definition?
4. What are the main drivers and benefits of BYOD for your company?
5. What is the main reason of encouraged UNDP to adopt BYOD? a. Is it economy reason, cost saving?
b. Is it Employees demand?
c. Is it Security reason?
6. What stage of BYOD adoption has been reached by your company?
7. How has BYOD adoption progressed compared to your expectations?
8. What do you believe is the number one inhibitor to BYOD adoption in your organization?
9. What are your main security concerns related to BYOD?
10. What is your biggest pain point when it comes to mobile security?
11. What negative impact did mobile threats have on your company in the past 12 months?
12. How is your mobile security budget going to change over the next 12 months?
13. Have any of your BYO or corporate-owned devices downloaded malware in the past?
14. Have any of your BYO or corporate-owned devices connected to a malicious WiFi in the past?

15. Have mobile devices been involved in security breaches in your organization in the past?
16. How long did it take your organization to recover from the mobile security breach?
17. What user group(s) does your organization enable BYOD for?
18. Who is responsible for setting BYOD policy in your organization?
19. Which of the following applications and use cases do you allow on Bring Your Own Devices?
20. Which mobile platforms does your company support?
21. How do you currently support BYOD users experiencing device / access issues?
22. Which risk control measures are in place for mobile devices?
23. What tools does your organization use to manage mobile device security?

24. What challenges have you encountered with Mobile Application Management (MAM)?
25. In your opinion, what key capabilities are required for Mobile Threat Management solutions?
26. When an employee leaves (regardless of reason), what percent of the time do you actually wipe their devices?
27. When employees leave the company, what device data removal processes do you use?

Interview Transcription:

Skype interview with Ognjen Krstulovic who is the head of ICT unit in UNDP Bosnia-Herzegovina where he had been working for almost 20 years.

00:00:00] My name is Ahmad, I am a student, master's student of Aalborg University in Copenhagen. And right now, I'm, uhm, uhhhh, writing my Master's thesis uhhh which is about BYOD security. The security risk associated with BYOD and uhhhh, economic impact of BYOD on the company's economy. So, and I had, I had an interview yesterday with your colleague here in Copenhagen, and he said that you are, you are more practically working on BYOD in Bosnia and Herzegovina.Is it...? [00:00:46] Ahmad, I might need to explain in which uhhh, manner and at what dimesion we have used the BYOD here in UNDP Bosnia and Herzegovina because it might be a bit

misleading.[00:01:05] Yes.[00:01:07] Uhhh, we have done, we have basically implemented Bring Your Own Device, for the only, for the mobile phones. [00:01:16] Ok.[00:01:17] And..[00:01:17] Yes.[00:01:18] And the, when we, when we have been implementing it, it was mostly related to the fact that we, uhh, we used to purchase mobile phones for our staffs.[00:01:34] Yeah.[00:01:35] But then we offered them an option that uhhh, we don't purchase phone for them but they were eligible for uhh, kind of a refund for the purpose that they uhh, purchase or use phone that they own, that they pick by themselves. [00:01:59] Ok. yes. [00:02:00] So, even for the (pause) view to the, I would say economic reasons, not as much, many people have decided to use that option.[00:02:10] Ok.[00:02:11] Because the funds were not uhh, extensive and they could get, we still put uuuhh, telephones, mobile phones for about 60 percent of people. [00:02:24] Ok. [00:02:25] OK? [00:02:26] Yes.[00:02:27] So yeah. That's, that was a good intro about what you have done so far. [00:02:32] In terms of computers we, we are actually on the other side of spectrum, we dont really uuuhhh, uhhh, we don't let our staffs let our staff use their own computers.[00:02:46] Yes.[00:02:47] In, uhh, for, for most of the business purposes. They are, we do have guest while it's hard to spare, one can bring their own device in work but they are very limited in terms of what can be done and how it can be done.[00:03:02] Alright. [00:03:03] Uhh, uhh while at our network.[00:03:06] Ok. [00:03:07] But, yeah you ask questions now and I'll be more specific for whatever you want to know [00:03:13] Alright. Ok, sir. So, first, first question is of course, I want, I would like you to introduce your name and your job position in UNDP. [00:03:24] My name is _____, I'm head of ICT Unit in Bosnia and Herzegovina.[00:03:30] Ok. And how long you are working in UNDP? [00:03:33] I'm working in UNDP for almost 20 years. [00:03:37] Alright, that's a long time. [00:03:40] Yes. [00:03:41] So, if I would ask you about BYOD definition, what, how you define BYOD in your opinion, in your...[00:03:50] BYOD can be, I define it in two ways, [00:03:55] Yes. [00:03:56] And I think it's usually how it is, BYOD can be defined as an...company policy or attitude towards allowing, allowing staff to use their own computers for work and then providing the means to use their own equipments for work at the office or even from home. On the other hand, I, I, when I think of Bring your Own Device I also think of, of it as matters of, how would I put it, as a method of quiet

management. [00:04:44] Yes. [00:04:46] Where one spectrum of the, of the, of the, you have managed devices, which I have them manage and provided by company, on the other hand side, you have user-managed devices. [00:05:02] Yes. [00:05:03] Ok? [00:05:04] Yes. Then, I would like to ask that, what are the main reason that encourage UNDP to adopt BYOD, is there any, do you know any reason that if you are..now you have just for the mobile device part, some management, but, but, what would be the main reason that you are, you are thinking to adopt BYOD in UNDP? [00:05:34] For there are number of reason of, number of reasons, let say number, so one of the reason is a people, users' satisfaction. [00:05:48] Yes. [00:05:48] as users might be happier to use the device that they have picked up by themselves [00:05:54] Yes. yeah. [00:05:55] rather than what is given to them. [00:05:57] Yeah. [00:05:58] Then, user efficiency [00:06:00] Yes. [00:06:01] as users might be, might use equipment they are used to, better, [00:06:08] Yeah. [00:06:08] and more efficient than something that they received from the company and they are not quite accustomed to [00:06:15] Yes. [00:06:16] What else? There is a reason of , on the management side, you could gain, you could gain, ease of maintennace or much less maintennance of the devices if, users are responsible for the management of the devices. Or servicing them or getting another one if it break but the, there's also a ____to it because it can also generate much more work for IT Unit because if there is a system where ITT Unit provides for, to manage devices, then it's much easier managing standardize devices, it's much easier than if you have, _____ environment where everybody gets, gets you to fix them, their equipment which you, which comes from various vendors, etc,etc. [00:07:30] So, what you, what I understood that you mean is, the main reason is assets management in the, within the organization.[00:07:37] UH..uhm. [00:07:38] would be one main point and, and the employees self-efficiency and confident to work to use on their own device. [00:07:49] There is also one important thing which relates to UNDP is in particular [00:07:56] yes [00:07:56] which is that UNDP is a, is a, I'd say, I'd name it fertile organization to implement BYOD.[00:08:05] Yeah. [00:08:06] Because most of our systems are web- based [00:08:12] Yeah. [00:08:13] Most of our systems are, uhhh, centralize, just a second excuse me..[00:08:24] Yes. [00:08:25] Uhhh, so most of our

systems are centralize, so in terms of, if you have propriety systems they are, that are accessed through the internal networks, and if you want to allow your staff to work from their computers, you have to install software on their computers. You must be sure what kind of, what degree of security is implemented in their computers, if they are managed well, if they are updated, etc.etc.[00:08:54] Yes. [00:08:55] But,but, for UNDP most of the applications are web-based. [00:09:02] Yeah. [00:09:03] and centralized so, it, it, you don't really have to do much at client computers to enable people to work with our ERP or with the intranet or etc, etc, which might not stand for many others, organization [00:09:23] Ok, so if I ask you the same area, about the main reason, is there any economy reason involved? For the cost-saving and all of those stuff? [00:09:37] Well, there, there might be but, so, why would, economy reason would translate in ICT Unit having to provide last words to the equipment. [00:09:51] OK. [00:09:52] With the administration of the assets would be less [00:09:56] Yeah. [00:09:57] But it's also a too prank thing where you might end up with more work. So, in terms, of course you don't purchase equipments.[00:10:08] Yeah, Ok. [00:10:09] But, on the other hand, in our example, we had to kind of, some kind of, monetary support to do to people, to purchase their devices.[00:10:24] Yeah.[00:10:25] Or, it was not much, you wouldn't be able to buy, uhhh, you wouldn't be able to buy a sophisticated phone or something like that but if you have one, you could offset the cost of it. [00:10:42] Yeah. [00:10:43] Ohh, I'm sorry I don't know what is it today. uhhhmmm, so, just, one second, where were I, so in terms of, we have done, we basically offered people the same amount of money as we have spend, we have spend for purchasing one of the phones we've got from the mobile phone company and it was fairly cheap to us. So, for the, in our example, we don't have much of an economic gain by introducing BYOD for the mobile phones so..[00:11:31] Ok, so let me dig little bit deeper in this manner because you said you provide the same amount of money to the worker which they purchase mobile phone by themselves and then in this case who own the device if you provide money to buy, is it for the user themselves or you named it that UNDP own this device? [00:12:05] Uh, for this particular case we have device policy [00:12:10] Yeah. [00:12:10] we basically, uhh, user owned the device. [00:12:15] Yeah. [00:12:14] OK? [00:12:16] Yes. [00:12:17] And we have provided the financial, what's this, subsidy for them. [00:12:26] Yes.[00:12:27] But, it was

very limited and if we have provision such as, if a person leaves an organisation after a year, they have to refund this money and that kind of thing [00:12:42] But, but the, they, do they should refund the full price the money you give or is there also discount of percentage because if they use this device for a period in the company and of course..yeah [00:12:56] They we have,for us, as the amount of money they received was, in around 100 euros, a bit more [00:13:05] Ok. Yeah.[00:13:06] For us, it would be much more complicated to, to do the accounting and retrieved [00:13:15] Yeah. [00:13:15] minute amount of money. [00:13:18] Yes.[00:13:19] So, we just put it as one year break down funds, [00:13:24] Ok. [00:13:23] if you pass one year, you get, you don't have to refund anything, but if you're less than one year you get to refund the whole amount at stake [00:13:33] Ah. Ok. [00:13:35] But the device was and through, through the purchase was always yours [00:13:41] Yeah. Ok. because according to the economy saving about the BYOD, you know, the earlier device that company's provided to the worker it's, it's a old fashion device and now it's new modern mobile devices which they work as a computer so, in this case if, if, I just want to explain a little bit about that, if the company provide a new device, it will, I believe that it will cost a huge amount of money, for example now you provide only 100 euro or maybe little more, so, the device which is cost much more than this, and the life cycle of mobile in this modern, modern time that it's very often would be change and in the case of BYOD if there will be any hole, backhole and, and, vulnerabilty inside the operating system then you need to provide another device or, or, or, upgrade it and so on, so this are all cost for the company. So, the, in this way, I'm thinking that of course if you are not impemented BYOD strategy for long period you cannot see this kind of cost saving, and I know this because I'm researching more about that maybe, it would be little bit sudden for you or, or, surprised for you. But, in this way, I'm thinking that there are some, some cost saving. there should be some cost saving or more expending money because on the other hand then you need to implement some technical like the device management, mobile device management solution which is provided by some, some provider... [00:15:54] yeah. yeah. [00:15:55] software provider and so on and your technical department should take care of the devices and so on, and having courses for the, educating your worker how to use the system and so on. These

are all costs. So, there is cost saving and cost, so, at the end, at the end of the day, then you, the, the company should "look ok, I spend this amount and I save this amount" then you will find out that ok, it's worked or you saved more or you spended more. Of course, it will not, it will not be find out by only short period. So, I, that's what I was , i was meant in the, in the, in the asking about cost saving but, but the beginning of the point that now you asa UNDP, you put the price of the device or especially mobile in the user side, right? Just.. [00:17:02] In the user? [00:17:03] Yeah. Because you just provide 100 euro and they are the one who, who buying their own. [00:17:09] There's a bit of a difference [00:17:11] Yeah? [00:17:12] with what we have done because we were like [00:17:15] Yeah [00:17:15] early, adopt this and we have done it before the global policyhad been iontroduced. [00:17:22] OK. [00:17:23] I think in the global policy of UNDP, it's not really allowed to provide this kind of monetary subsidy for users to, to, to, to get the, to purchase their own device. [00:17:39] OK. Yeah. yeah. Ok.[00:17:41] And for us, it was a kind of, we wanted to achieved is that, within a certain period of 2 or 3 years, we get to a situation where we can say, where we can stop buying cellphones. [00:17:59] Yeah. Ok.[00:18:02] And we would just provide sim cards and mobile phone numbers to users and they would then purchase any phone that they would like. This is kind of significant, it can be viewed from two sides, it is a significant saving, in terms of just purchasing phones but at the other hand it's not that much and sometimes we are just willing to pay for it to insure of some level of a, of a staff satisfaction [00:18:44] OK. [00:18:45] And on the management side, we have an experience that firs of all, when having a contract, and the life span of both contract and cellphone is around two years that's what we aim for. It, then we,, the we get significant discounts and we get for this 100 euros a bit more, we get really decent android mobile phone so we, and the, at some discussions we had internally, it might be even easier on the management side to just get all the mobile phones by the company and if somebody needs it fix, if it breaks or something happens you just replace it. [00:19:41] Yeah. yeah. Ok. So, I want to ask also, do, how many staffs you got in this department in Bosnia Herzegovina? [00:19:54] Well, we are, we are kind of 230 people operation [00:20:01] Yes. [00:20:02] Whereas, about sev..60 people are, 60 persons are authorize to get, eligible to get a cellphone, [00:20:12] Yes. [00:20:14] and then out of it,

I think 15, 15 or something have been using, BYOD instead of the company phone. [00:20:24] Ok. 50 or 15? [00:20:27] 15. [00:20:28] 15. Ok. Ok. Yes. So, we can jump to the next question, uhh, yeah, that's I, I think I got all, nearly the answer, what, what stage of BYOD adoption has been reached by your company, so it's partial, so far, I see is a partial implemented, right, adopted like..[00:20:57] Yes, yes. [00:20:58] Yes. Ok. And the, How, how has BYOD adoption progress compared to your expectation, did you expected more to be adopted or it's ok that's what you expect? [00:21:20] Basically, what we have done before we have implemented this, we have asked people [00:21:25] Yes..[00:21:26] In a kind of a survey what, what they would go for, [00:21:28] Yeah. [00:21:29] And there was a bit, I think, at the beginning there was a bit larger about 20 percent of people were, were up for the refund [00:21:41] Yes. [00:21:43] But then, when we announce of how much refund would be,[00:21:47] Yeah. [00:21:48] because they have probably expected that we would provide them with, i don't know, 250 euros or something. They have figured out that they can get better phone from the , from, from UNDP than they can get if they get, if they use money to buy one at the market. It's also a bit constrained in terms of that, usually you can strike a better deal with a telecom company if you have a contract. [00:22:23] yeah. [00:22:24] and the, with this bring, where UNDP pays for a mobile phone cost, not the phone cost but conversation cost and subscribing cost, you, you have the mobile phone detached from that contract, so you cannot get savings or, or, [00:22:46] discount, discount [00:22:48] you cannot pay of the 2 years, you have to pay upfront and stuffs like that. [00:22:53] Hmm Ok. [00:22:54] So it's a bit, so, at that point, when the actual implementation went up, I think the number reduced to 10 percent. And then over the time, we have, I think it went back to bit about 15 percent of, in total because some people got their phones broken or they got themselves new ones that they like better and that's about it. When we are discussing it both internally and with the, with the colleagues who use phone, I'm not really sure what would be , what would be the way for work. I think we still enable some kind of hybrid approach where we would like, allow people to use the mobile phone that they purchase but still, I think we would have to maintain a number of purchase phones for UNDP. [00:23:53] Yes. So, then , now we come to next question, I think more or less, I can, I can find the, the answer but I will ask

anyway, what do you believe is the no.1 inhibitor to BYOD adoption in your company? [00:24:12] ahhh, uhhh, I think it's a, it might sound strange but I think the main inhibitor is the practice and actually tradition. [00:24:29] Ok.[00:24:31] So, if we would established a completely new office, it wouldn't be that complicated to tell people, that these are the rules that we will follow so, i dont know, we will provide you with mobiles with cellphone numbers and you are suppose to get yourself a phone or even if you can, could translate it to computers you could say, ok this is now, you are free to purchase the computer, you might get subsidise you might not, I don't know it depends on the, on, on the policy and we, we ain't gonna service, we will provide you with some kind of assistance with the system that UNDP provides. With that kind of approach, you would be able to have, I think high rate of Bring Your Own Device adoption. But in the position we have now, is that taking a, some people don't see them receiving mobile phone from UNDP an entitlement which you are striping, stripping off, you know. and then you have a certain resistance. Then there are options with what people can do with these phones, they are not technically limited to, to using their phone. They can, if they have a better phone, they still can get one from the company and give it to their family member. It would be very hard for us to figure that out. So, the, the, I think it's more of a tradition that prevents us from, because now, to switch to Bring Your Own Device in total, would have some negative consequences, in terms of how our staff reacts to it. [00:26:32] So, next question comes to the security, what are your main security concern related to BYOD, if you, if you have some security concern? [00:26:44] We as UNDP, as I said we have a fertile situation where Bring Your Own Device is not as dangerous as it might be in some other companies [00:26:58] yeah [00:26:59] But, most of the threat of Bring Your Own Device are covered with the policy not with the actual security measures [00:27:11] No. Ok. [00:27:12] Because, Ok, I'll just mention some, and most, I think the key, key issue, so lemme, let me, I'm just trying to, to, to structure it a bit [00:27:27] yes [00:27:28] So, if the mobile device is not within the private network, number one security problem for you would be virus infected devices [00:27:39] Yes [00:27:40] But, if you're implementing Bring Your Own Device when you do not have to have internal network, where all the devices can be co, can be connected to some kind of a internet connection that parallels one in a internet cafe or in public space where each devices protecting, protected towards

itself, you don't have to worry much about that. Then, what you have to worry about is how users authenticated to your central web-based system and if you have a good, good authentication, this if you fllow up the industry standard which UNDP probably does then it doesn't really matter because anyways you don't know if a person connects to your ERP or the, well you know but you don't really care if the person is connecting to your ERP from their own device, at the office, at home or internet cafe or wherever in the world. So, so, you don't really take that in consideration, are you there? [00:29:01] Yes. [00:29:02] And the greatest threat that we drill up to is, what happened with the data on these devices? and this is very hard to, to, to control by any kind of tools or, or because what people do and specially an organisation that are not strict with policies and the technical means to prevent it, is that you have, you get your data wander all around the place. It's on the cloud, it's on a private cloud drive, it's in a usb stick, it's in your phone, it's with, it's get copied number of time and we through the policy and the global policy adresses it somehow transfer the responsibility for the data at the device to the user. So, and it's again more of the policy thing than to what, what happens in reality, so user is supposed to wipe clean their device, when, when they, when they want to get rid of it, but if it actually happens it's a completely another, another story. Then, and the only, how would I say, the only provision that would allow tools to interfere with what, what had been with the users device is that within the policy, it is written that in case of flaws or theft of the device, UNDP will remotely wipe the device. [00:30:46] Ok [00:30:47] OK? [00:30:47] Yes. [00:30:48] And, I'm not sure if that happened already but, then there you have two stories; one is, if user really, in some cases, user really wants to do, to wipe the device, so they would come to UNDP and UNDP will provide the service, which should by the way down through the Office365 and it's a convenient way because we already have Office365 so we don't have to employ addidtional management staff, software to do that.[00:31:20] Ok.[00:31:21] And the, on the other hand side, the reason, situation where user loses, lost the phone or it was stolen but it was never reported so you don't, you don't really wipe it and you don't know what happens, what happens to the device, what happened to the data. Might be important to say, it, this as , this what I have said doesn't actually apply only on mobile phone, it would apply on any user-owned device with UNDP system's access but for the cellphone, it is

to implement for the private personal computers, it would be very hard to implement [00:32:12] Yeah, i understand. Ok, so next question, I think, yeah I got the answer already because you said you haven't, you haven't observe any kind of this situation which they will ask for wiping and you don't have any registered like this, because the question is; what negative impact did mobile threat have on your company in the last 12 months, so, you haven't got any stolen or lost devices to wipe it or something like that? [00:32:49] We had.[00:32:50] Ok.[00:32:51] And, as I, as I remember there was one device, most of the devices were broken, but there was one stolen device and I can retrace bit of a story to you because it is, it also relates that there is a quite a need for bring your own device education to us users, what happened in that users has is the device or, it was stolen at the very first moment what they did is they've change the password. [00:33:24] Yeah. Ok. [00:33:25] So, when they changed the password they made it impossible to remotely wipe the device.Because the device was accessing UNDP system through the, through the password that was stored, used earlier and stored in the device. So, the story is that basically what you should do is you should first inform the ICT and we could then initiate the wipe of the device,and then only after that you could, you could, you could what, change your password. [00:34:02] Ok, So why in this case can you, if it's in the policy, you can just block the, the what do you call the account of the user of the mobile phone so he will not, it will not have a connection or, or, it can not establish anymore connection with the UNDP but int his case the data in the mobile, then, you, it could be unmanageable and..[00:34:32] For you to send the wipe common to the device, the device has to log on to UNDP system [00:34:38] Yeah. So..yeah so, you have observed also this kind of situation. [00:34:48] What?[00:34:49] You have, you have had some mobile threaten because you, your staff have lost the, the mobile phone and, yeah that's happen, you have this case already. [00:35:03] Yes. yes. [00:35:03] Yeah. Ok. [00:35:04] So and, the next question, how is your mobile security budget going to change over the next past, next 12 months, do you have specific budget, security budget to doing those things? [00:35:22] No. no. We don't have that any kind of, of budget, made for this specific of thing. And it wouldn't change much for us, because the way I would implement bring your own device is a..by not...by..is again through the policy but not through significant investment in any security. In any security, to, or measured. As I said

UNDP can do that, some other organisations probably cannot and if you really analyse it...the only, if you chose to implement tools to manage privately owned devices..it would probably cost you as much as managing your own device, company owned devices, if not even more. [00:36:33] Yes, ok, So, next, I have 2 questions basically they are so similar, it's, if you have observed your corporate device or even company owned device downloading any malware or malicious wifi, have you observed any in the past? [00:37:01] No. not really. [00:37:04] Not really. OK. So...[00:37:07] But we also do not mix..mobile devices that users, user-owned in terms of network security, they connect through a separate wireless LAN which, which basically has only connection towards internet. [00:37:29] Ok. So..and..but there's also a wifi malicious if they have any, if, for example if they connect in, to the wifi in some public places and they transfer..come back to, to your your, your, your company and connected to the wifi again, it's very possible to bring malicious, wifi malicious and the..and..[00:37:54] I'm not sure , if I understood you correctly but there is a, we have number of different wifi network within the office [00:38:06] Ok. [00:38:07] So, one is the secure one which we use for our laptop computers where you get most of the access, ok? But the laptop is secured in different manner. and then you can connect your cellphone to the other network but that, that would allow you only to browse web and you wouldn't be able to access internal company system through the network. [00:38:34] Ok.ok So, in this case then next question is talking about the involved security breaches so if, if it's not allowed to connect to the internal network so that will not happen as well, that's what..[00:38:49] yeas, that's, that's the way we would wo it by the way [00:38:55] Yeah.[00:38:56] If you want the device to connect to private network then you really have to manage huge number of security aspects including software updates, the, the, the software application installed in the device etc, etc. [00:39:14] Exatly. [00:39:15] It becomes quite expensive thing to do. [00:39:18] Yeah, it's more complicated and, and, yeah. So if, if we come to talk about the recovering a mobile, mobile when it's lost or breached or. or, any kind of these security issues, do you, it, would it take long time to recover or not? [00:39:47] How'd you mean? Can you ask the question once more? [00:39:51] Yeah. [00:39:52] The, the just for not. Basically, all the rules for the privately own device , they kind of apply to the UNDP owner, owned device it's, it's more or less the same. [00:40:04] Ok. Yeah. Ok. This one is if, if

this question is in the case if the, if the staff will use the moobile device for all the purpose of the work then, then, I'm looking for it would be difficult or how long it will take to recover if it is, if it's in the case of the device breached or lost or stolen all of those stuff, to recover the data in it and, and solve the problem, but in the case if only staff using as, as a normal device, mobile cellphone and only browsing in the internet, so, so that, there should not be that a lot of data placed in the device..[00:41:06] The key of UNDP way of doing it likewise globally is that whatever we do can be cloud based [00:41:14] Yeah, yeah. [00:41:16] It's 99 percent of the sync, so our emails, our documents, our intranet, our financial applications, it's all that day, so basically you don't, there is no reason for you to store any data at your device you just use device to access and , access the system and use the data over there. [00:41:39] Ah, ok. Yes. [00:41:41] So, it's a great plus in terms of Bring your own device, you don't have to really worry about the data at the device but as users are not educated that much of course some data is downloaded to the device, so, some data is, at a certain point is used at the device, it wouldn't stopped, in essence, you could just give any other device to users and they should be able to continue working immediately. [00:42:13] Yeah, yeah OK. So, the question is, one question is what, what group of staff does used or enable BYOD in your organisation?Most of them..[00:42:29] How'd you mean which...[00:42:31] What [00:42:32] As, as, what if I can..[00:42:34] What group are enabling BYOD because as I remember you have 230 people in you..[00:42:42] Well, the people who are eligible for some phones are usually managers of sort, or certain staff that might need or might have a..did we..where they work require them to use phone more than normal but of all the people I would say that it's more related to the habits of the people and more, people who are more technology savvy and interested in trends they would probably go and buy themselves a new and better phones than what we want to provide them with the, with the, UNDP provided phones which is worse than the ones they already have. So, they would up for the BYOD.[00:43:45] Ok. Then if I ask, if I may ask who is responsible for setting the policies and all of those stuffs in the organisation for all those devices? [00:44:00] How'd you mean policy for devices? When you mean policy, do you mean written policy or the security policy? [00:44:09] Yeah, security policy. [00:44:09] For the user-owned devices we do not set anything. [00:44:13] No? [00:44:14] We provide assistance in terms of how

would you connect your email and stuff like that. [00:44:17] Ok. But the policy for the organization who will be responsible, is it IT department or the main department? [00:44:26] Yeah, In terms of security policy IT department would implement them. In the UNDP globally, there is a policy implemented to security policy which is applied whenever somebody logs on to the email globally. [00:44:43] Hmm. [00:44:45] So, there is one. In terms of written policy, we do have a department within, globally in UNDP that devices IT security policies but for the , for our approach we have our own policy deviced because it happened before the global policy was issued.[00:45:04] Ok. Yeah exactly, because what I hear, what I remember from the interview yesterday in the department here, they say, they have no, against any people which they bring their own mobile phone, memory stick, hard disk, they plug in, in the computer whatever they want to do they are free. They don't have any restricted policies against them. [00:45:33] Yeah yeah. well, we have a bit of extensive policy in terms of personal computers that we deal with, in Bosnia Herzegovina. UNDP, as you might know is a bit different in each country. So, in UNDP Bosnia and Herzegovina, we do have a kind of heavy list policy compared laptops and pieces. [00:46:00] So, the, and one question I think is not so relevant, I want to ask what, what, what mobile platform prefer UNDP to the staffs but I think it gives, it gives to the staff, them totally free what they bring, right? [00:46:19] Yeah.[00:46:20] yeah, ok. [00:46:20] Yeah. Well the policy just, the written policy has just requires people that they have functional phone that should be updated by the latest update and they should obtain the software that is required to connect to the UNDP system would be basically that they have their mail client and Office365 but most of it, they can do without it. [00:46:49] So, if I may asked the, the, if there's any experienced issue would the device access lately in, in your department, is there any issue when the staffs*s coming for the accessing to the internet and stuffs like that, is there any issue? [00:47:15] How'd you mean, can you rephrase it? [00:47:17] Yeah, because, when the staff bring the device to the company, they have access to the access point you give and they have a communication between themselves, I don't know how is, how is the network configured but is there any issue to communicate and access to the access points and those stuff? [00:47:41] Oh, when, users pay, it's pretty basic really, it doesnt, it, they have a, there is a common password and they just

connect to it. [00:47:54] So, there's no any issue there? [00:47:56] No, not really. [00:47:56] Ok. Then, which risks control measures are in place in your mobile device? But, I think, you..yeah because the way you implement it, is not like a..there's three kinds of BYOD implementation, one is only internet access, and one is partial and one is fully. I think your, in your case, it's only internet access. [00:48:26] Yes. yes[00:48:28] So, then in this case, there's no measurement control and all of those stuffs, I think is not included. So, do you have any tools to, within the organisation to control and manage the devices and the securities? [00:49:01] (mumbles) Can you please repeat the question..[00:49:02] yeah, do you have any tools, for, for within the organisation to control the mobile devices and the securities? [00:49:11] We actually do.[00:49:13] Ok.[00:49:14] So basically, the very first tool that is currently implemented and used by the UNDP globally is Office365. It's a basic thing, it doen't really provide a lot of function, but it does provide some of the options as enforcing a password complexity, device lockouts and the, the you can do a device wipe. [00:49:35] Yeah. OK. [00:49:38] We in Bosnia Herzegovina, we also have a Microsoft system centerconfiguration manager which is supposed to be able to do a bit of a mobile management, but we don't use it for that purpose. [00:49:55] Ok, so...[00:49:56] I think globally is pretty same situation, we do have a configuration manager but is not used for the mobile phone management. [00:50:04] So, you don't use any kind of mobile, mobile device management tools for managing? [00:50:12] Just, just as I've said, Office365. [00:50:13] Just Office365, this is, actually this more for the, for enforcing the policies something like that..[00:50:22] Yeah, yeah. Oh, you mean in terms of, yeah, configuration manager is more, more of the tool that you, you would ask for. You was asking, but we do have it but we don't use for the purpose.[00:50:34] Ok. So, in your opinion what key capabilities are required for mobile threat management solution? [00:50:50] Capabilities for mobile..?[00:50:52] Yeah. For managing, for threat management solution..[00:51:01] Well, uh, it's a bit difficult question but uh, to be able to manage client devices you need to have, a, the, first, a software that is able to operate on various devices' operating systems etc. so, it have to be really, uh, how would I say, there should be really extensive number of platform that it must work on. Uhh, what you will have to be able to do is, you will have to know the levels of the software to enforce

updates, to know if the device are compliant, to be able to install or uninstall software, and to be able to have some information on what data and, what data and how much of it resides at the, on the mobile device. [00:52:06] Ah, ok. So that's basically, there are some, some mechanism software which is, like mobile device which means mobile application management and all of those stuffs so..but if you haven't, if you haven't implemented fully functional of BYOD then..[00:52:29] Uhmmm, yeah. Yeah. [00:52:29] So when, for example, when an employee leaves regardless if, doesn't matter what's the reason, how long it will take to wipe or remove the data on his device, her or his device? Is it easy or take long time? [00:52:50] It is very easy thing to do. It is just a bit of, how would I say, there is no, it's uncertain process. Basically, it is, i think even users should be able to wipe their devices by themselves. I'm not sure about that, but it's usually a one-click operation for administrator [00:53:24] Ok. [00:53:25] But if it's gonna happen, uhm, if it's gonna really wiped the device, this is a question that I, I cannot, so let me see... yeah, I can even, i see when I log on to my website, I can see all the devices that used..all the devices that used to connect, that have been used to connect to my email but, I can wipe them from the, from the webmail basically. [00:54:22] So are you capable to do it remotely or you need to have the device physical? [00:54:30] It seem that I should be able to do it remotely. [00:54:34] Remotely? OK. So, the next question is almost answer, what, when employees leave the company what device data removal process do you use...this is the wiping, right? You, you...[00:54:54] Yes. [00:54:55] You..in both cases you can do physically and remotely, [00:55:00] We haven't really done that, no.[00:55:01] No? Ok you haven't really done that...no..Omgen, it's the last question and it's not really question but, it's asking your opinion if you can add more which is important that I forgot to asked related to the risks with BYOD and BYOD economy impact within, to the organisation and in general, if you have anything to add or to suggest to me, base on your experience 20 years working in this organisation..[00:55:47] Well, in my professional, how do I say, outlook, if i look at things kind of strategically, for me, it's more of a question, uhhmm, uhhmm, when mobile phones are discussed and mobile devices it's kind of a lightweight Bring your own device, what really matter and make significant changes to organisation is, if you transfer that to personal computers up to the actual equipment where the work has been done. And, for

me it is the greatest question which, which way it's better to go either to keep the managed devices or to, to try to implement the, the fully pledged bring your own device, BYOD program across the organisation. Whereas the, whereas there is a bit greater for opportunity within UNDP because of the way UNDP is, is a, of the way UNDP has its applications where they are online, they are authentication only, etc.etc [00:57:13] Ok. So, now, it's pop up the last question, is not in my schedule but I just want to ask, do you think in the future you will implement fully BYOD functionality or..[00:57:31] The honest answer is, I don't know because this 20 years of experience has really taugh me, well not taught me but we had an approach where people using their own computers were, had the strict policies at their computers where they are not able to and still not able to install software on their own and it, it was probably one of the key factors that we didn't have any major security incident throughout this period. So, giving up on that wouldmean that there is something else that is a..how would I say? That is much better than that. Now, the, there is a bit of a thing I wanted to mention, it's kind of an organisational maturity to switch to bring your own device and it's, if, we on UNDP would want to do so..we would first need to make sure that really all of our system, that we don't have internal systems that we can protect computers each for their own and then it's whole different type of system that would be in play. And we are now, not at that point yet, we still have internal network where we still don't have file servers and file shelf, once we got rid of that, we might be a step closer to a proper bring your own device. On the other hand, you do have to know, that it is also a bit of an economic thing and for person in US or UK or in Denmark where I suppose that you already have a laptop computer.[00:59:40] Yeah. [00:59:40] And a tablet and a mobile phone before you start working or started working. It might be a thing of choice. But in Africa or even in Bosnia herzegovina if I get a person employed, they might not have enough money to own a computer. [01:00:01] yeah. That's correct. Ok sir, I would say thatnk you so much for your time and for your cooperation. [01:00:08] You're very welcome. [01:00:09] And I wish you the best day and I appreciate it. i appreciate your time too. [01:00:16] I have a strange, a bit strange request for you, is it possible that if you have recorded the converstation, is it possible that you, that you have, you send me the recording? [01:00:28] Yes, I will try my best. I have recorded and I will replay it again if it's recorded properly and good then I will,

I will keep in touch to you how I can manage to send it to you. Yeah, I will do that. [01:00:45] Ok. It would just interesting to me because you have driven me in a process of rethinking stuffs so, I can, reuse my answers if I will put it this way. [01:01:01] Ok. yes. [01:01:02] Thank you very much. [01:01:02] Thank you. Thank you so much and I appreciate it. [01:01:05] You're very welcome. [01:01:07] Thank you bye. [01:01:09] Bye. ###end