CHAPTER I

INTRODUCTION

1.1 Introduction

The uses of mobile devices such as laptops, tablets, and smartphones have increased in today's businesses. Mobile devices have been used for both personal and business purposes. These have led to a new concept known as "Bring Your Own Device" (BYOD). Most organizations allow employees to use their own device which relieves some of the initial costs of acquiring and licensing the devices. Such a policy also supports more productive and technologically demanding workforce (Morrow, 2012). According to a survey made by Johnson & Filkins (2012), more than 80% of employees use some types of personally owned devices in the workplace. One of the advantages in allowing employees to bring their own device and use for work is that it increases efficiency and flexibility. By giving access to the company network, work can be done from any place and at any time. Also, BYOD increases the speed of work as well as customers satisfaction because of perfect communication and quick reply. However, some organizations start worrying about the security risks that are associated with BYOD far outweighs the benefits (Morrow, 2012). One of the biggest challenges for organizations are company data being entered to devices that are not managed by the IT department, that has security risks of data leakage and data theft (Cavoukian, 2013). Various threats by enabling BYOD such as loss of smartphones will lead to loss of data, allows unauthorized users to

read and also leads to prejudice the device and other applications that did not managed by IT department.

Employee awareness towards BYOD security is still limited. The employee uses his or her personal device for work purposes without aware of the security consequences that can be occurred. Employee's errors could threaten the company's data from leakage and corruption. Many organizations have tried a variety of policies to allow for BYOD in their organization with limited success. Organizations should find a flexible policy to secure BYOD environment. IT department should have a new approach to balance the device preferences of the employee with the security requirements needed. This policy allowed employees to use their own devices with certain rules, such as the specific applications that can be accessed to the organization network, control the access based on user role and job description in the organization. Also, inventory authorized and unauthorized device access on the network. All these requirements can mitigate the attacks that might reduce the security level in organization. Another essential part to succeed the business is employee awareness on BYOD, most security issues in work environment occurred via employees' error because they are not aware enough about the policy that the organization put it.

1.2 Bring Your Own Device Concept

Bring your own device is a program which allows employees to use their own mobile devices for work purposes via access to the internal network of the organization. The first goal of the BYOD program is to enable an employee to be more efficient and give more services through the choice of

the device that is preferably used in business purposes. While ensuring at the same time the safety and security of information (Cavoukian, 2013).

Figure 1: Bring Your Own Device Concept

According to Scarfo (2012) BYOD is used to describe the employees whose bring their mobile device such as laptops, tables and smartphones into the workplace for both working purpose and also personal use. Bring your own device concept allows an employee or user to bring his mobile device to company or working environment to implement work tasks. As the increase in mobile and internet users it becomes more common to have a smart phone with networking features. This concept is also useful because of many features such as easy to use, accessible from anywhere and anytime as well as low cost devices (Kulkarni et al., 2014).

The 'D' in BYOD includes more than just smartphones or tablets. It also includes employees logging into web applications such as Outlook Web Access and SharePoint, SaaS applications such as CRM systems, from home

laptops, smartphones that connect to companies networks which increase threats to the sensitive data for the organizations. Organizations should be concerned about the risks that may occur. Keyloggers, Malware and cyber-attacks have really increased the risk from unauthorized access, and unmanaged applications (Morrow, 2012).

1.3 Bring Your Own Device Security Concerns

According to Tokuyoshi (2013) network switches the arbitrary remote has put of corporate data at risk. Without protection in place to secure network traffic. Private information such as a postcard is open to anyone to read. If they made an endeavor to look. With the appearance of modern technology such as smart phones and tablets which used in the workplace, it became the vast majority of employees using these devices as a primary business tool. Thus, the employee merges personal data with business data in the same device. This trend called bring your own device, and became using widely in companies all over the world because of its efficiency and high quality to raise the level of performance of the work. But also introduced new types of security risks in business.

According to Gajar et al., (2013), conducted the sale of very large for smart phones compared with personal computers PC. This device has become more widely used for business. There are more than 5 billion mobile phones, access the Internet and various mobile applications that make users more prone to cyber-crimes. Smart devices and mobile phones easier to loss and theft, and that can claim to steal data. Another reason for risk of BYOD is the

result of the exposure device to malware. Most mobile devices are not properly protected from malware.

According to Miller et al., (2012), when an employee uses a personal smartphone or tablet in the workplace, it makes concerns to worry about security. For instance, external (personal) devices are attached to the company network; malware could migrate from the personal device into the company's devices and over the company's networks. In the other direction, sensitive information is likely to make its way onto the personal devices. This information may include customer data that should be kept private and company information that should be kept proprietary. When that kind of information walks out the door on a daily basis, bad things can occur, especially if the device is subsequently lost or stolen.

1.3.1 Specific Risks and Concerns

- **Untrusted Network**

Mobile device easy to attacked because most of organizations have no control over the security of the external networks. Public communication and wireless system such as Wi-Fi and cellular networks can be susceptible to eavesdropping and man-in the middle attacks (Ketel & Shumate, 2015). There are some strong encryption technologies used to protect the confidentiality and integrity of communication such as virtual private networks (VPNs). Encryption on data should be applied on both data in transit and data at rest. Data that have been sent over unsecured mobile networks can be problematic, especially when they sent by unencrypted way,

it can be viewed by anyone connected to the same network, directly or indirectly (Shumate & Ketel, 2014).

- **Lost or Stolen Device**

Using mobile device for work purposes can be a big risk, whether is owned by the employee or the company, in case the device is lost or stolen. This is may cause a great issue when personally identifying or confidential client information is downloaded to the device (Shumate & Ketel, 2014). There are many techniques used to prevent unauthorized access on mobile devices and can be help with dealing with the loss or theft of the device. First, lock codes or passcodes used to lock the mobile device and require a password, and pin or preset action to unlock the phone. From these types of techniques are a password is the most secure. There is a geo-tracking can help in locating the device when a smartphone is lost. Geo-tracking also includes the ability to remotely lock and remotely wipe the mobile device (Ketel & Shumate, 2015).

- **Malware**

Malware has become more common issue in era of technology along with mobile device use. This is appealed especially on Android devices, which includes about 51% of all of the smartphones in the United States. There are many efforts tries to combat this problem on mobile device (Shumate & Ketel, 2014). According to McAfee Labs, 80% of the mobile malware is specifically targeted at Android devices (Ketel & Shumate, 2015). With the proliferation of malware targeting mobile devices and increase of cyber-

attacks, it is considered a source of great security concern when these devices related to business system. There are many types of malware for example, Trojan horses and key loggers.

1.4 Problem Statement

In the past years, the use of mobile devices was not very common in the workplace. The employees in companies and establishments had no choice only to use the company's devices such as computers and phones. Nowadays, mobile devices specifically smartphones have become more peryasive in most of the organizations. The employee brings his or her own device and use it for work purposes. This phenomenon leads to many of security concerns in work environments. For example, the employee loses the device or the device is stolen, which lead to data leaking. Losing the information because of employee's error can compromise data and the security of the device as well. Malicious software (malware) also can threaten the security of the device and data (Miller et al., 2012). On the other hand, device resources are very limited such as processing power and battery life, where it is very difficult to trust these devices to access to private information (Chung et al., 2012). To mitigate this downside, we need to set a number of the security policies commensurate with mobile devices. Many researchers are focusing on security risks for BYOD (Georg & Carsten, 2013; Madzima et al., 2014; Scarfo, 2012; Shumat & Ketel, 2014). But less attention has been focused on solutions for BYOD security, furthermore, the current BYOD frameworks addressed BYOD security solution to a single and specific problem, none of these approaches are able to fully addressing the issue of BYOD. Therefore,

this research proposes BYOD security framework as a solution that enhances the security in the BYOD scenario without compromising the usability and flexibility of the system.

1.5 Research Questions

The research questions that will be used in this research are as follows:

1- What are the elements needed to propose BYOD security framework?

2- How to propose a framework for BYOD security?

3- To what extent the chosen elements of BYOD security framework are acceptable?

1.6 Research Aim

The main aim of this research is to propose a new framework for BYOD security.

1.7 Research Objectives

The research objectives of this research are as follows:

1-To identify the elements of BYOD security framework from SLR.

2-To propose a new framework as a solution to secure BYOD.

3-To evaluate the acceptable of identified elements in BYOD security framework.

The table below shows the summery of research objectives, research questions and methodology used.

	Research Objectives	Research Questions	Methodology
1	- To identify the elements of BYOD security framework.	- What are the elements that needed to propose BYOD security framework?	-Systematic Literature Review
2	-To propose a new framework as a solution to secure BYOD.	- How to propose a framework for BYOD security?	-Systematic Literature Review.
3	-To evaluate the acceptable of identified elements for BYOD security framework.	- To what extent the chosen elements of BYOD security framework are acceptable?	-Interview

Table 1: Summary of the research objectives, research questions and methodology used

1.8 Significance of the Research

The increased use of personal mobile devices in business through the technology era led to the worsening of security risks. These risks can affect the success of the business. The main significance of this research is to helps the organizations to how to make BYOD securing with flexible use. To that end, this research presents a solution to the "Bring Your Own Device" issue

in organizations that adopting this phenomenon through propose a new framework to secure BYOD.

1.9 Scope of this Research

The scope of the research:

1-The research focuses on security policies to secure BYOD in organizations.

2-The framework built based on 2-tier of security control along with device security profiles, anti-malware scanner, user role, user profiles and applications control.

1.10 Research Contribution

This research contributes towards:

1-Reveal the elements that needed to secure BYOD environment.

2-Develop a new framework as a solution to secure BYOD environment.

1.11 Thesis Structure

This thesis contains five chapters, including the introduction. This section is briefly reviewed these chapters as follow:

Chapter 1: Introduction. This chapter gives a background about this research which is bring your own device concept and the security concerns about this trend. Also, describes the problem statement, the objectives of this research, research questions and significance of the research are explained briefly.

Chapter 2: Systematic Literature Review. This chapter presents a systematic literature review related to BYOD security policies. This chapter also summarizes the existing studies on BYOD security policies.

Chapter 3: Research methodology. In this chapter the methodology that has been used in this research is described.

Chapter 4: Findings and discussion, BYOD security framework was formulated based on systematic literature review and the interview findings are discussed in this chapter.

Chapter 5: Conclusion and future work, summarization, limitations of the research and suggestions for future works are discussed in this chapter.