CAPTER II

LITERATURE REVIEW

2.1: Introduction

The purpose of this quantitative and correlational study was to assess the security awareness level of smartphones among Zawia University students. The result from this study provided insight into students' smartphone security awareness and trust. Students who owned smartphones, aged 18 or older and attended one of two departments (science and literature), were invited to participate in a smartphone security awareness study. Demographic data such as gender, age and academic specialization were examined in relation to the level of smartphone security threats. The security awareness level of smartphone threats was also examined to the relationship with the smartphone security features.

This chapter discusses available studies on smartphone security awareness and security training. For further understanding on the concept of the security awareness, this study shows related studies related to smartphone security threats, smartphone security features and information security awareness.

2.2: Smartphone: An Overview

Smartphones are part of our daily life. Using a smartphone nowadays has far exceeded the use of computers. Smartphones combine functions of mobile phones and computers. 1973 experienced making the first device that combines phone and computer. First Smartphone was released to the public in the 1993 which was produced by IBM. The term "Smartphone" first appeared in 1997. Smartphone can be defined as a handheld mobile telephone device that integrates advanced information processing functions with conventional mobile phone capabilities. The smartphone can be defined in many ways:

- Elgan (2007) defines the smartphone as a portable device that combines a wireless phone, email and internet access and organized into a single, integrated piece of hardware.

- Gartner (2009) defines the smartphone as a large-screen, voice-centric handheld device to offer complete phone functions while simultaneously functioning as a personal digital assistant.

- Litchfield (2010) examined the top five most accepted definitions of smartphones, and concluded that there was no single, accepted definition due to the constantly evolving nature of mobile phone technology. In conclusion of

his research, he defined the smartphone as that "runs an open operating system and is permanently connected to the internet".

With a large number of products equipped with touch screens, Smartphones characteristically offers users the ability to customize their handset as they please, enabling unrestricted installation of desired applications in much the same manner as PC. Smartphones offer functions that are not available on PCs, including HD video cameras, GPS devices and other accessories, and in light of this, Smartphone allows people to stay connected to internet networks and easy to check their emails. Smartphone provides document reading capabilities, are able to process, store and transport information, they are used by workers as working tools (Allam, 2009).

There is a need to be mindful of the fact that although Smartphones offer a high level of convenience, there is always the possibility of new risks emerging as a result of this convenience factor. Also the applications for Smartphones are not as powerful as on the regular computers. Popularity of smart phones is constantly growing together with a number of third-party applications and Smartphone applications, such as Google play and Ovi store, according to (Mylonas et al., 2013).

Mobile phones are very useful in our daily lives, as older people in Malaysia confirmed that the importance of mobile phones lies in emergency situations and when they were in trouble (Nizam et al., 2008). On the other hand, there are also a few disadvantages to these Smartphones, one of these disadvantages is the attack by malicious softwares and often these malwares are distributed through electronic store applications because of the minimum control measures on the content it provides. Even with the antivirus products, firewalls and security software, it's still difficult to

find 100% secure network. Sadly, the biggest damage in these cases is Smartphone users. The greatest danger lies in the inappropriate users' behavior fed by mixing of personal and business use. As a result, managers and security professionals must educate their customers (Landman, 2010).

The smartphone is a ubiquitous device among university students and had a profound impact on their lives. Access to social media sites, such as Facebook and Twitter, and features as texting have captured the attention of the students, and many students spend a considerable amount of time utilizing these features (Brandt and Heller, 2007). Using smartphones by students in classroom is a major challenge to most professors. Also, many universities have issued written policies to this effect.

2.3: Smartphone Security Threats

The smartphone is exposed to different security vulnerabilities, threats and risks due to their capability to access open networks. From the previous studies, vulnerabilities, threats and risks can be defined as follows:

- Vulnerabilities: defined as an "identified weakness of the controlled system in which necessary controls are not present or are no longer effective" (Whitman and Mattord, 2004).

- Threats: defined as "attempts to forge, steal or gain access to the system by manipulating, sniffing, or redirecting data transmitted across the network" (Dhillon, 2007).
- Risk: defined as “a product of the probability and impact of threat against the information assets of an individual or an organization. Also the threats exploit one or more vulnerabilities” (Whitman and Mattord, 2004).

Symantec Corporation (2011) on the Internet Security Threat Report found that, from 2009 to 2010, the number of new vulnerabilities in the smartphone operating system jumped 42 percent. The number and the complexity of the attacks on smartphone are increasing, and the countermeasures are slow to catch up.

According to (NPD Group, 2011) about 40% of users of smartphones are worried about threats such as viruses, hacking and credit card security, more than one-third are worried about harmful applications and malicious electronic mails as well as concerns regarding user's location. 82% of smartphone users don't have any security software products on their smartphones; nearly a quarter of this percentage considers security products as very expensive; the majority of consumers are reluctant to pay for security software products.

Jeon et al., (2011) divided threats into two groups; threats caused by attackers and threats caused by user unawareness or intention as shown in the Table 1.

Table 1: Security Threats

Threats caused by attackers	Malware
	Wireless Network Attack
	Denial of Service
	Break-in
Threats caused by user unawareness	Malfunction
	Phishing
	Loss
	Platform Alteration

This study pays more attention to the second type of threats which relates to user unawareness. These threats can be defined as follows:

Malfunction means: the smartphone application can malfunction by incompatibility between platform and application.

Phishing means: the user can expose his/her private information by accessing the phishing site, messenger phishing or by SMS phishing.

Loss means: the user can lose his/her smartphone.

Platform Alteration means the user can alter his/her smartphone platform intentionally e.g. rooting in Android operating systems.

This quantitative research focused on assessing user awareness level on these threats. Based on a report published in December, 2010, by ENISA (European

Network and Information Security Agency), the main risk of smartphones is user unawareness. Smartphone applications have a privacy setting for controlling the location from where data are transmitted, however, they are unaware of the existence of the privacy setting which prevents transmitting data and the probability of being infected by a malware. Smartphone users can install malware into their Smartphones unwillingly; the malware includes SMS, MMS, SPAM mail and other various ways. Also, when Smartphone is lost or stolen is one of the main threats. This report showed the types of the widely spread threats such as, data leakage resulting from device loss or theft and unintentional disclosure. Actually, 56% of respondents did not know that failing to properly log off from a social network app. Could allow an imposter to post malicious details or change personal settings without their knowledge. And 37% were unsure whether or not their profile had been manipulated.

2.4: Smartphone Security Features

Advances in technology mean that the smartphone provides services and features similar to desktop or laptop computers. These smartphones offer many new ways to communicate and capture and disseminate media. And usually support a wide range of functionality; web browsing, email, voice and instant messaging over the internet, capturing, storing and transmitting audio, video and photos, enabling social networking, banking and many other activities. However, these activities introduce new security issues and increase existing risks. Significant research has been conducted in order to secure smartphone devices (Anderson and Agarwal, 2010).

Meanwhile, security measures such as antivirus and encryption are uncommon on smartphone operating systems. Also, not updated as frequently as on personal computers, according to the National Institute of Standards and Technology Report (2013). Mobile social networking applications sometimes lack the detailed privacy controls of their PC counterparts. Unfortunately, many smartphone users do not recognize these security shortcomings. Many users fail to enable the security software that comes with their phones, and they believe that surfing the internet on their smartphone is safe. Also, not updated as frequently as on personal computers, according to Trend Micro Report to smartphone users (2009). This research focuses on smartphone security features which can help the users to secure their smartphones. The following is a review of some smartphone features:

Screen lock: one of the most common basic security features is a screen lock, which enables a user to protect access to their devices by automatically locking the device whenever the screen is turned off. Screen locks are similar to passwords used to log into a computer and are based on the methods that fit within the different usage patterns of smartphone devices. Keeping a smartphone device secure is considerably more important. Because smartphone devices frequently are a gateway to a wealth of sensitive data. Bruggen et al. (2013) studied phone locking and the behavior of users with these features. Also, this study found nearly one third of users did not lock their phones. That was very worrisome from a security perspective.

Encryption: it is a high security feature, the information on smartphone device can not be looked at without entering the PIN number. If the smartphone device was lost or stolen, a thief might be able to attach it to the computer and look at

the contents. By encrypting it the smartphone owner prevents any access unless enters the PIN (Burgess Computer, 2015).

PIN Code Number: (Password or Personal Identification Number): is a simple way to keep unauthorized users out and is the first line of defense in the case of smartphone got lost or stolen. When enabling the PIN protection, typically selecting a timeout period, this allows the smartphone to automatically lock after the selected timeout which offers greater protection (Burgess Computer, 2015).

IMEI Number: (International Mobile Equipment Identity) Each mobile phone has an individual serial number called the IMEI number. Which can be identified by the mobile phone service provider's network. The users should record their IMEI numbers in case of smartphone got stolen or lost. IMEI consists of a number of fields totalling 15 digits. All digits have the range of 0 to 9 coded as binary coded decimal.

Thieves have been deterred from stealing smartphones with the introduction of IMEI blocking. Blocking an IMEI on mobile phone networks prevents a smartphone from being used with any SIM on any mobile network (Garda National Crime Prevention Unit, 2012). Based on the importance of these features as basic security of a smartphone, the author decided to study the users' awareness and trust on smartphone features.

Virus Scan: Nowadays, many people uses their smartphone to browse the internet. The smartphone can be prone to a malware infection. But most users have not yet considered making use of an Antivirus software to protect their devices. Viruses

can be harmful to the operating system of the smartphone, applications, personal information and contacts. They can put the smartphone at risk, such as Data loss, corrupted files and OS and convey private information without the user's knowledge. There are many viruses-scan software such as Kaspersky, McAfee, Symantec and F-Secure.

Anti-Spam: The Anti-Spam component can block unsolicited calls and messages on the basis of custom (black) and (white) lists. When the white list mode, Anti-Spam delivers calls and SMS only from numbers included in the white list.

2.5: Smartphone Security Training

Academic institutions face more challenges when it comes to securing their systems due to the complexity of their information system (Burd et all, 2007). Rezmierski et al (2002) state "The nature of the teaching-learning environment requires a vast array of operating systems, platforms and networks to meet the need of various scholars thus increasing the complexity of the overall system". Rezgue and Marks (2008) point out that universities are targets for attacks because of the high computing power and open access they provide to people within and outside of their institutions. Universities are among the least secured information systems, and few of them conduct awareness training.

Although most organizations are recognizing the importance of user awareness programs, they do not fully implement them. Katz (2005) also points out that the universities are prone to many of the potential human threats to information security

due to the amount of confidential information being handled at any given time. Payne (2003) affirmed that "prevention in the form of education and awareness programs can help campuses avoid serious security ills".

Training techniques that engage students are effective at decreasing security risks. Software developed at Carnegie Mellon for Wombat Security Technologies shows that it is possible to train students to recognize phishing attacks. This software (PhishGuru) distributed mock phishing e-mail attacks. Also reported that, the people are more willing to play games than read training materials, and games have been shown to promote long-term retention. The anti-phishing tips and strategies take only a few minutes to absorb and are presented in a fun cartoon format. Carnegie Mellon plan to extend this training for other types of threats.

2.6: Information Security Awareness

In any organization around the world, the most valuable are the people that are the main basis for an organization to succeed. Security awareness is significantly important to reduce data loss. User's awareness has to be taken into account because it is the foundation upon which the success of mobile-related services are based. There are a lot of theoretical studies about smartphones that focuses on user's awareness using statistical ways. They often use questioning techniques to collect users' opinions. There are many surveys in this area focusing on mobile phone’s security issues.

The awareness is a component of the education strategy of an organization which tries to change the behavior and patterns in how targeted audience (e.g. Employees, students, general public) use technology and the internet and it is a distinct element of its training. It consists of a set of activities which turn users into the organizations' first line of defense. There are several information security awareness definitions presented below:

- Cincinnati State (2013) defines the "information security awareness as educating the campus community about the inherent risks of the confidentiality, integrity and availability of systems and data, and how we all can protect these systems and data".
- Wilson and Hash- NIST (2003) defines information security awareness as "awareness is not the training, the purpose of awareness is to focus on the security, and to enable users to recognize the security threats".
- Veseli (2011) defines the information security awareness as "the level of security awareness based on the knowledge and attitude, as well as understanding of information security, and the readiness to act and behave according to it".

From the above definitions of information security awareness, and the importance of the smartphone security features to ensure the basic security of the university students from the security threats, the author decided to study the awareness of the smartphone security features and the its influence on awareness of the security threats.

2.7: Study Factors

This study focus on five factors that may be contribute to user awareness level in smartphone security. These factors were (gender, age, educational level, academic specialization and smartphone experience). The factors were stated as the following:

2.7.1: Gender

Several security awareness studies reported the gender factor. The studies were inconclusive about the gender effect on smartphone security awareness. Some studies concluded that males were more secure than females (Mensch et al., 2011). While other studies contradicted this by stating the men were more risky in their security than women (Jones et al., 2012). Finally, No research has been identified which definitively indicated one gender was more secure than the other gender. Further research is necessary to make this determination.

2.7.2: Age

Age factor was reported in nearly every study. However, the predominant age groups varied across studies, each study received a larger sampling of one age group over another age groups. The research were inconclusive regarding a correlation between age and security (Mensch et al,. 2011 and Riola, 2014). Mensch et al (2011) found the students aged between 18-23 were most compliant with security than other age groups.

2.7.3: Academic Specialization (Major)

The studies were inconclusive regarding a correlation between the specialization and smartphone security. Some studies found a correlation between the major and smartphone security (Androulidakis, et al,. 2010) (Mensch, et al,. 2011). On the other

hand, other studies found no correlation between major and smartphone security (Grajek, 2013).

2.8: Gaps in Literature

Many studies on smartphone security awareness have been conducted over the past decade, yet cybercrime continues to grow. The human has been identified as the weakest link to security, the researchers have attempted to understand the factors such as gender, age, educational level smartphone experience as they relate to security awareness. The smartphone are growing faster than any other technology and are quickly becoming the target for cybercrime. Also the wireless is prevalent on college campuses. The smartphone devices which can access the internet and also more exposed to security threats. Several security awareness studies reported the gender, age and academic specialization factors. The studies were inconclusive about the factors effect on smartphone security awareness and these research as reported in Table 2. Mensch et al (2011) concluded that males were more secure than females . While Jones et al (2012) contradicted this by stating the men were more risky in their security than women. Furthermore, the research were inconclusive regarding a correlation between age and security (Mensch et al,. 2011 and Riola, 2014). Some studies found a correlation between the major and smartphone security (Androulidakis, et al,. 2010) (Mensch, et al,. 2011). On the other hand, other studies found no correlation between major and smartphone security (Grajek, 2013). Therefore, it is very important to gathering more information about the level of security awareness and how the factors influence the level of security awareness.

Table 2: Summary of research

Factor	Researcher	Finding
Gender	Mensch and Wilkie, 2011	Males were more secure than females
	Jones and Heinrichs, 2012	The males were more risky in their security than female
Age	Mensch and Wilkie, 2011	The students aged between 18-23 were most compliant with security than other age groups.
	Riola, 2014	The age group don't effect security awareness.
Academic Specialization	Androulidakis, et al,. (2010)	Academic specialization effect the security awareness.
	Mensch and Wilkie, 2011	
	Grajek, 2013	Academic specialization don't effect the security awareness.

2.9: Summary

This chapter has presented the review of some information security studies and shown the border view of the research area. This chapter has highlighted the importance of smartphone security features to ensure basic security to users, and some security threats threaten users because of their low awareness level. Also, it highlighted the security training. Finally, it presented some statistical results from previous studies which are related to the research area.