

CHAPTER II

INFORMATION SECURITY AWARENESS

2.1: Introduction

This chapter discusses available studies that are designed specifically with the purpose of creating awareness in order to educate secondary school students about information security awareness. For further understanding on the concept of security awareness, definitions related to the specific term are presented. Related studies are also discussed and broken down into several subsections as: information security risks, security awareness training program, evaluation of information security awareness, information security challenges and success of information security awareness. All of these topics are to create deeper understanding and to stand further on the needs of our study.

From the literature, it can be summarised that information security awareness is a multilevel process where the user needs to move from one step to another. In our study, the focus area is “security awareness and security practices”. The overall classification of information security process is described in Figure 2.

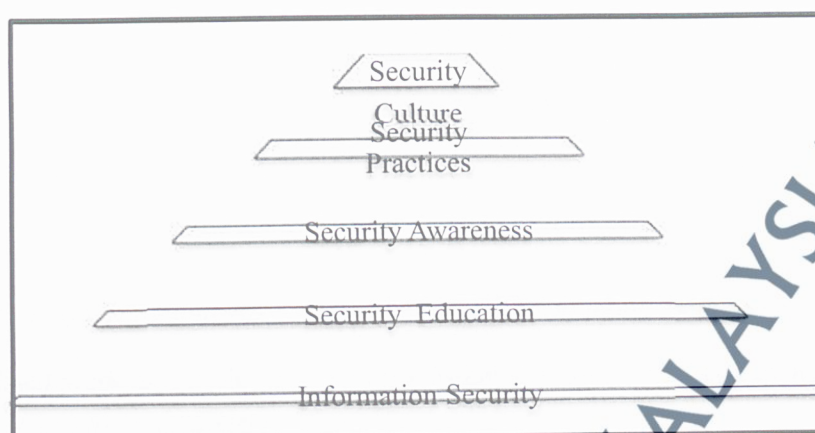


Figure: 2 Classification of Information Security

2.2: Information Security Awareness Definitions

The basic goal of information security awareness is to have a real positive impact on the employees' behavior (Veseli, 2011). Information security awareness has many definitions. Below are some of the definitions defining the term "Information Security Awareness".

- "Information security awareness is educating the campus community about the inherent risks of the confidentiality, integrity, or availability of systems & data, and how we all can protect these systems & data" (Cincinnati State, 2013).
- Talib (2014) stated that information security awareness can be defined as "initiative to enhance user's behavior toward information security practices by distributing related knowledge of security awareness".
- Wilson and Hash- NIST (2003) defined information security awareness in the article of "Building an information technology security awareness and training program" 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".

- Shaw et al., (2009) defined security awareness “the degree of users understanding about the importance of information security, and their responsibilities toward safeguarding the information, and some of risky practices”
- Veseli (2011) summarize the definition of information security from other related work 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, the definition can be summarized as “the state of educating secondary school students to ensure they recognize the security risks and their role of strength their personal information”.

2.3: Related Study

This section focuses on the previous studies that have been conducted by others that are closely knitted to information security awareness. Although not all of these researches are specifically targeted towards secondary school students, it is important to study them in order to investigate what has been conducted, scope covered, and to find out an effective way to meet the objectives of this research.

2.3.1: Information Security Risks

The vulnerabilities associated with the use of the Internet bring about many risks to different users. Being part of Internet users, secondary school students are also not spared from facing various risks that can cause information lost or any kinds of threat for their personal information.

Alhejaili (2013) stated that cyber-bullying becoming a serious threat that affect secondary school students negatively. The author also listed different kinds of risks that children may suffer from the online services as showed in Table 1.

Brady (2010) stated that as the Internet expose children to wide risks, children might not have the skills, abilities, and knowledge to control these risks. Brady found that children use Internet for playing games (77.95%), looking up information (40%), social networks (22.56%), and making new friends (9.74%).

In addition, Brady (2010) had added security risks to the list of content, contact, and conduct risks. As Brady stated, the security risks could be applied to children from the nature of the Internet as viruses, spyware, spam, identity theft, disclosure of personal information and phishing. In the same study, the National Center for Technology in Education (NCTE), conducted a survey in 2008 on children's use of the Internet, it noted that children have a significant increase in the use of instant messaging, number of children providing personal information, and the use of social networks as daily activities.

Table: 1 Cyberbullying Potential Risks

	Commercial	Aggressive	Sexual	Values
Content (Child as recipient)	Adverts/ Spam Sponsorship Personal info	Violent/hateful Content	Pornographic unwelcome sexual content	Bias/Racist Misleading info
Contact (Child as participant)	Tracing Harvesting personal info	Being bullied, Harassed or stalked	Meeting/ Stranger Being groomed	Self-harm Unwelcome Persuasions
Conduct (Child as an Actor)	Illegal/downloading Hacking/gambling Financial Terrorism	Bullying or Harassing another	Creating and uploading Inappropriate Material	Providing Misleading Info/advice

A report cited by Smith et al., (2006) defined cyberbullying as “Forms of bullying using electronic devices such as mobile phones, emails, or text messages. Cyberbullying, have become more prevalent with the increase conservation of technology. This report took place in 14 different schools in London, focusing on the age of 11 to 16 years old. The report employed a quantitative methodology via questionnaire, with some qualitative sections. The authors classified seven types of cyberbullying as follow:

- Text message bullying
- Picture /Video clip bullying (via mobile phone camera)
- Phone call bullying

- Email bullying
- Chat room bullying
- Bullying through instant messaging
- Bullying via websites

This report assessed some factors, such as the awareness of different forms of cyberbullying, the comprehended impact of various kinds of cyber-bullying compared to the normal bullying, and finally, examine the age and gender differences. The finding of this report suggests that bullying is happening more outside of school compared to inside. Furthermore, this study found out that among the types of cyberbullying, 'text messages', 'phone call bullying', 'email bullying' were the most common forms. The report indicated that the gender has high different, as girls are more exposed to cyber-bullying than boys.

Another definition cited in Belsey (2012) stated that "cyberbullying involves the use of information and communication technologies to support deliberated and hostile behavior by an individual or group that is intended to harm others".

Donegan (2012) in a report on cyberbullying and its history, prevention and analysis. He stated that "the technology has evolved, bullying has proliferated". With the increase concern of youths on chat rooms and Instant Messenger (e.g. AIM), teens are now able to communicate with each other without any limitations. According to the results from Donegan study, he found that there is a difference in the average based on the past few years (From 2004 to 2010). Furthermore, he denoted that the Internet and cell phones are the primary tools used for cyberbullying. Moreover, he also stated that gender has its impact on cyberbullying as girls more likely to be involved in cyberbullying in all of its categories. Finally, he stated that cyberbullying has

permanent mental effects as this could reflect on the suicidal thoughts and violent response by teens as a result of dangerous effects. He recommended having prevention programs as this program need to “clearly identify the problem, establish recognition, and formulate consistent ways of dealing with the issue across all platforms”.

Faryadi (2011) discussed the effects of cyberbullying among 365 students of Universiti Sains Islam Malaysia (USIM). His argument was based on the emotional and physiological effect of cyberbullying upon students’ academic performance. Questionnaire, interviews, checklists, and observation were deployed to obtain the results from students. The majority of 35 (13%) of respondents had suffered emotionally due to cyberbullying, while 255 (70%) agreed that bullying adversely affects students’ academic performance. He suggested that “institutions, teachers and parents must realize that cyber space is a risky place and must take effective steps to protect the victims”.

Dueck (2006) stated that the Internet has a negative face while providing a threatening space to users as the personal risks. As he discussed, the Internet is now no longer the place which is free from prejudices of race, gender, and ability. He further showed that in traditional bullying, children can escape by hiding in their houses, but now cyberbullying is happening inside their rooms. He further discussed that the victims of cyberbullying are the same of traditional bullying and they are singled out just for being different. The author summarized from other surveys that Cyberbullying has increased toward teenagers in its frequency and severity and the girls are the victims in this risk.

Cyberbullying stories are other evidence that gives us a clear idea of the danger which could result from the cyberbullier. For example, a fourteen year old female called

Justine, was way beyond scared when she discovered that she was a victim of cyberbullying. She started receiving threatening email messages to the extent of 90 messages in the box held. The contents of the messages were ranged as dangerous, such as “I’m going to rape you”. The parent took action by going to the police and the results showed that her best friend were behind the entire story (MAB, 2014).

Another story showed the real face of the damage caused by cyberbullying when Nadia hanged herself in her bedroom after she received an avalanched of abuse by trolls telling her to “kill yourself”, “nobody wants you” and “you are not normal”. All of these messages were when she broke up with her boyfriend and she chose to go to the “Ask. Fm website” to have a new sympathy (Mackay, 2014).

Around 2,212 teen male and 2,162 teen females were involved as a random sample in a study of cyberbullying. The results showed a difference in the sample ratio between boys and girls as found in these three areas:” Victimization within a person’s lifetime (16.6% for males and 25.1% for female), admitted to a cyberbullying offense within a person’s lifetime (17.5% for male and 21.3% for female), and had a hurtful comment posted about oneself online (10.5% for males and 18.2% for female. The results reported that males reticence about admitting a past bullying experience (Hinduja and Patchin, 2010).

Li (2006), surveyed 246 students from three junior high schools in China. He reported nearly half of the students have been engaged in cyberbullying, while one in four had been cyberbullied. Also, gender showed a significant difference as males were more likely to be the bullies and cyberbullyies, and females’ cyberbully victims were more likely to inform adults than female.

Social networks could be described as “A web-based network which is designed for users to construct public or semi-public profiles for self-expression and social interaction, articulate a list of other users to share connections, view or traverse a list of connections and those made by others within a bounded system” (Boyd and Ellison, 2008).

Alhejaili (2013) stated that social networks make it uncomplicated for people around the world to have a source of communication and interacting with others. Users from different age groups login into social networks and share their daily activities. O’toole, (2011) stated that “on a typical day, 70 percent of teens ages 12 to 17—17 million teenagers—spend from a minute to hours on Facebook, MySpace and other social network sites, according to the National Centre on Addiction and Substance Abuse (CASA). Children may face risks related to disclosing about sensitive information via social networks as this information resulted in increasing their vulnerability to undesired contact (Brady, 2010).

Nauert (2011) on a report on the legal risks associated with the use of social networking sites as experienced by 1000 secondary school students, teacher and parents in Australia. The most popular site among students is Facebook with the majority of 93% of students using it. Moreover, the author reported that majority of students update information on their social networking sites at least every day. Furthermore, the surveyed students indicated they have received unwelcome or unpleasant contact by strangers via their social networking profile. On the other hand, some students are concerned about security risks, such as identity theft, and other about privacy or unwelcome disclosure of data.

Livingstone (2008) conducted a qualitative study, by interviewing 16 teenagers aged from 13-16 years old in their houses. The sample consisted of 50% boys and 50% girls. The aim was to identify the risky practices by teen via their social networks accounts based on (e.g. Myspace, Facebook, Bebo, Piczo, or similar which they had visited at least once per week). She stated that “creating identity and social relations online is not only time-intensive and, on occasion, risky, but it can be difficult to manage”. As part of the finding, teens face problem in managing their privacy online. Furthermore, teens prefer to express their personal experience via these websites.

The majority of 64.5% of social networks users indicated that they sometimes share their daily activities including pictures, while 11.8% always share their activities finally 23.6% indicated with never. This finding was as a result of conducting a survey on 150 secondary school students in United State of America (USA) (Alhejaili, 2013).

Another risk was mentioned by Alhejaili. When the sample was asked if they sign-off from their social networks after finishing the work as this can lead to the illegal use of their accounts by intruders. The results showed that (32.4% sometimes, 21.9% no, while 7.6% indicated that they do not believe it is necessary to sign-off). This can cause the misuse of their profiles or even posting unpleasant content under their profiles.

A report on the danger of social web showed that teens often disclose about personal information when they need to get acceptance from their peers. Moreover, this information when posted online can be seen by everyone. Teens also tend to appear popular by posting the details of their weekends when this information can reposted by others in an unwanted way (Wave, 2007).

Padric (2012) surveyed secondary school students aged from 16-18 years old in Grahamstown. Part of this study investigated about the use of password habits among students. This aspect was measured to assess the level of awareness and the risks among the students. The results showed that students have a slight level of awareness in term of passwords length. On the other hand, students showed bad passwords practices as reported they “never change my passwords”. The overall results reported that the level risk was high.

Teens aged 14 to 18 years old reported as they are sharing personal information. One of the teens shared her password with a stranger for an online gaming site and the result was paying for lots of the gaming site (Sterman, 2012).

Harley et al., (2005) surveyed secondary school students in UK schools. The study concerned different security risks such as “virus, worm, internet safety, passwords, and web scam”. As part of the finding, students appeared to have a little idea about computer security and they know how to pass the parental control.

Based on discussed security risks, we find that there is a real need to assess secondary school students’ awareness level regarding social networks, cyber bullying and passwords. Moreover, to stand in the perfect way to find out the exact method to educate students about security risks.

2.3.2: Security Awareness Training Tools

People are listed as the weakest link in the chain of information security, as any potential risks could result from human faults. In order to reduce these risks one of the important mechanisms is the security awareness training of employees (Eminagaoglu et al., 2009).

NSIT- 50 in a report of building an information security awareness and training program and to introduce the awareness training program as “an awareness and training program is crucial in that it is the vehicle for disseminating information that users, including managers, need in order to do their jobs” (Wilson and Hash, 2003).

A video game called (Cyber CIEGE) was deployed in a security awareness training program in the US. This game was provided for free non-governmental organizations. The two important scenarios of this game focused on Navy IA training requirement “Make the player aware of basic IA problems and principles, and intended for more sophisticated users of computer-based assets”. The results showed that Cyber CIEGE game added an effective addition to basic information awareness training program for general computer users (Cone et al., 2007).

Peltier (2005) stated that “an effective information security program cannot be implemented without implementing employee awareness and training program”. Based on the case of our study secondary school students are the core age, which needs a concern on rise security awareness.

Veseli (2011) measured the effectiveness of information security awareness before and after conducting a security awareness training program. The training program was based on the following three categories:

- 1- Classroom
- 2- Discussion- based
- 3- Web-based training style

The results reported that each of the training styles has its advantages in improving the awareness among participants. Veseli stated that the classroom training style is more

effective in improving the knowledge, attitude, and behavior, among the participants in all mentioned topics of the study. On the other hand, web-based training style gave a better result on the topic of social engineering. Finally, discussion-based training was better on the topic of incident response-whom to contact.

Video and quiz are another type of information security awareness training materials that were used in order to have a better understanding of the security issues with students. The video was based on the acting of students on homemade video. After the video was published by the university students, they are required to answer a quiz to obtain their understanding of the reported security issues (Sommers and Robinson, 2004).

Brady (2010) deployed two kinds of research methodology in a camping session for the primary schools, in order to have better results in measuring the security awareness training program. The campaign was based on materials that were summarized from other educational resources on security awareness, advice and information from other schools, and governmental organizations that develop security awareness for children. As a part of the finding, the campaigns proved its success and effectiveness in increasing children's awareness level.

Wilson and Hash (2003) in a report of NIST-50 have provided techniques that could be used for delivering training materials as follow:

- 1- **Interactive video training (IVT):** this technology supports two way interactive audio and video instructions.
- 2- **Web-based training:** for the distributed environments when the session can study independently and at their own pace.

3- **Non-web computer-based training:** the most popular technique, especially if the access to web-based material is not feasible.

4- **On-site, instructor-led training (including peer presentation and mentoring):** One of the oldest techniques and the biggest advantages of this technique is the interactive nature of the instruction (Wilson and Hash, 2003)

Eminagaoglu et al., (2009) conducted a campaign session through one year in an enterprise company in Turkey. The campaigns consisted of educational posters, animations and e-messages on the company internet, surveys and simple online quizzes. The author concluded that awareness training and campaigns have positive and effective outcomes in several issues such as passwords' quality and compliance with passwords policies. Furthermore, he stated that "there should be an ongoing awareness campaigns complemented with supporting materials". Finally, the author suggested to measure the effectiveness of any security awareness training programs to stand on the end user needs as having a survey on the chosen group that participated in the training program.

In order to reduce phishing attacks, Sheng et al. (2007) conducted a training for anti-phishing. The training was based on "playing game; reading an anti-phishing tutorial based on the contents of the game, or reading existing online training materials". Results showed that participants who played the game were better in identify phishing websites after 15 minutes of training compared to other conditions. Sheng stated that game based learning provide an interactive activity that motivate end-users for phishing education.

Payne (2003) stated that "prevention in the form of education and awareness program can help campuses avoid serious security ills". He addressed that each age group

needs to meet its special security messages. He divided the groups to Administration, Students and Parents, Faculty and Staff, Researchers, Health Care Professionals, Auditors, Campus Police, and Attorneys, IT Staff, State and Federal Government Relation Staff". The methods of delivering the security program vary depending on the audience, the categories of these materials are as follows:

- 1- Meeting Presentations and One-on-One Discussions
- 2- Handbooks
- 3- Online Quizzes
- 4- Security Web Site and Web Ads
- 5- Security Alerts
- 6- Handouts
- 7- Articles
- 8- Security Fairs, Conferences, Seminars, and Workshops
- 9- Videos

In the concern of which methods used for students "In his article university students". Handbooks, Online Quizzes, Security Alerts, Security Fairs, and Videos, where the most appropriate methods of delivering security awareness programs to students.

Based on the needs of our study, the author deployed "Non-web, computer-based training" such as games, videos, and poster for the purpose of investigating information security awareness among secondary school students.

2.3.3: Evaluation of Information Security Awareness

Fakeh et al., (2012) investigated academic librarians in three private colleges in Malaysia (Damansara, Shah Alam, Petaling Jaya). This study has identified four

factors that can influence information security awareness within the studied area. Also, this study deployed the quantitative methodology in order to investigate the applicable objectives such as identifying the level of awareness in this kind of organization and the factors that influence information security in these organizations. A survey was used in this study to obtain the answers from the participants. The factors were the policy of information security, education regarding information security, knowledge of IT, and employee's behavior.

A health institution became a necessary situation to provide the confidentiality of patients' information. The study was conducted in three Malaysian hospitals and the size of the target samples were 500 respondents. The survey results of this study show that when user's behavior towards information security is acceptable. Security incidents can decrease, and the effectiveness of information system's security can be increased (Humaidi and Balakrishnan, 2012). In the same term (Shaw et al., 2009), and in another journal to (Koskosas et al., 2011) stated that employees must practice information security to increase the level of awareness toward the successful information system in an organization.

Padric (2012) conducted a research on online threat awareness. The target group of this research is secondary school students in Grahamstown. The students were in the grades 8 to 12. The objectives of this research are to determine the actual levels of awareness, and the difference between these levels and self-perceived levels of the participants. The finding of an online survey concluded that secondary school students registered a high level of risks, as they are unaware of the online safety and security. These risks could be clearly shown in the information security, online privacy, and

indeed online safety. The author suggests having awareness, education program that did not focus only on the concepts, but on the awareness and behavior precisely.

The home computer users can be the biggest weakness in the circle of computer and information security (Howe et al., 2012). The home computer users have been tested in the U.S.A, and many factors were measured to see why security may not match the position and abilities of home computer users. The questionnaire results indicated that home computer users can have a real damage more than others. In particular, when they do not recognize the threats, or they cannot carry on their training due to the cost of security programs. Finally, the author found that users preferred the benefits of risky behavior, which is agreed with other related studies (Larose et al., 2005 and Good et al., 2005; Debatin et al., 2009). This study recommends to have a suitable security model and price to imitate the needs of users and their security cases, and to provide users with an alternative security for their important procedures.

Veseli (2011) measured the effectiveness of a security awareness program before and after conducting the training. This research took place in 327 employees of GUC (Gjovik University College) in Norway. The training is based on different styles, such as: a classroom-based style, discussion-based group style, and web-based training style, and all of this was in order to identify the effective security awareness program. An actual material took place in this study, and both pre- post questionnaires were deployed in this study. The results of the post questionnaire concluded that classroom training based style is the most effective training in improving the knowledge, attitude, and behavior of the responding.

Wanajak (2011) discussed the Internet Addiction (IA) as a new academic field. This research took place in Thai secondary school students in Chiang Mai, Thailand. The

sample size was 952 secondary school students. This study focused on finding a definition to (IA) as well as to investigate the spread of the Internet and its impact on secondary school students. The finding of this study concluded that the IA definition as it accepted from the Delphi panel is “Repetitive Internet use leading to abnormal behaviour which causes negative consequences to its users or others in the community in any way, such as psychological, physiological, behavioural, sociological or other important functional impairments”. The survey result of this study found that only 3.7% of Thai secondary school students are considered to be suffering from Internet addiction and they recorded some difficulties with school work, physical, mental health problems and relationship problems. The author suggests that society, governments, schools and parents have to work together to spread the awareness toward changing the behaviour of Thai secondary school students.

Beyer and Westerford (2010) found that the only way to establish security awareness is by starting education programs as soon as the youth start communicating with computers in early ages. In addition, the study explained the importance of the school to improve security awareness among students. This can be done by providing educational materials that are focused on understanding the risks of Internet through the daily practice on the Internet. As part of her study, Brady conducted a review of two relevant researches to obtain the risks children may encounter during their Internet usages. Also, a questionnaire was sent to students and their parents and teachers to assess their awareness level. A training program that was adopted from other related website that considered e-safety for European children to enhance children' awareness level. A questionnaire and observation were the method used by this researcher to evaluate the training materials' effectiveness.

Herly (2009) discussed how users will skip the security advice when its high cost. In the same term (Dhamija et al., 2006) show that even, the professional users can be victims. Rahman and Hidayah, (2009) develop a prototype to evaluate information security awareness level of teacher and student in Malaysian secondary school. The purpose of the prototype is to identify the level of information security awareness based on assessment model. A questionnaire results of this research showed that the prototype evidences its effectiveness in evaluating the students' awareness level. Table 2 shows the researcher studies and their methodology to evaluate information security awareness among different end users.

Table: 2 Method used to Evaluate Information Security Awareness

Researcher	Method of Evaluation
Fakeh et al., (2012)	Survey- Questionnaire
Humaidi and Blakrishnan (2012)	Survey
Howe et al., (2012)	Questionnaire
Veseli (2011)	Training Program Pre and Post Questionnaire
Wanajak (2011)	Survey
Bayer (2010)	Review two relevant studies Training program for e-safety of European children Questionnaire – Observation
Rahman and Hidayah (2009)	Questionnaire

Having understood the methodology used in the previous studies as in table 2, our study focused in adopting a training program from South East Asia cyber portals as the material provided by some of these countries are designed specifically for this age

(13-18 years old), as well as deploying a quantitative (questionnaire) and qualitative (observation) methodology to fulfil the research objectives.

2.3.4: Information Security Awareness Challenges

Crossler et al., (2013) focused on future challenges upon researchers and how to provide the exact way to users' behaviour to understand hackers' policies, and to deal with information security. All of these were tested on four group members. As a result of this study, they found out that culture, fear, improving information security compliance, and unmasking the mystery of the hacker world were the aspects that will fulfil the future behavioural information security research.

From elementary to high school, a total of 2447 students were investigated related to their level of awareness. The result was that the rank of awareness was high in ethical issues such as the use of file-sharing sites. On the other hand, they have a low level of knowledge about the rules. In this case authors suggest to have education subjects related to security awareness education, and related activities to improve student's positive knowledge of how they must use the Internet (Tekerek and Tekerek, 2013).

Aloul (2012) showed the need of security awareness in schools, universities, governments, and private organization in the Middle East by presenting the results of several security awareness studies conducted amongst students and professionals in U.A.E in 2010. The author advised that telecommunication companies, media, non-governmental organization, schools and universities should adopt a proactive instead of reactive approach toward security awareness.

There is a research focused on testing the vocabulary of information security awareness to measure employees' knowledge about the concepts of security and risks

of information security. This study focused on providing a vocabulary related to security and the risks on the Internet such as viruses, spyware, malware and firewall. Two different class groups of students at university in South Africa were used as a sample test. The result of this research showed that a vocabulary test was beneficial way. The simple and the basic analysis of the relationship between knowledge of concepts and corresponding behavior were 89% had a good idea, and 9% indicated that they will provide their personal details if requested by e-mail. In the case of this study, it will be good for any organizations that need to develop the level of awareness of their employees by using vocabulary training (Kruger et al., 2010).

Bulgurcu et al., (2010) the focus of this study was on the individual factors that cause the compliance or noncompliance to the requirements of information security awareness in an organization. The study shows that the theory can give the positive attitude toward employees. The study contained 464 employees. This study showed the importance of employee compliance with the instructions provided by the organization of information security awareness. Moreover, they also found that the employee's punishment is a deterrent positive action to reduce the negative disposition.

The future challenges are chained where it is increasing and becoming more complicated whenever the end user is unaware about the potential security risks that caused by their failures. Whatever time or place is, there should be a security awareness instruction to face any future challenges and this should not be limited to any age group to limit the gap of awareness in any organizations. The three security risks that are presented in our study (passwords, social networks, cyberbullying) draw another challenge in front of children as these risks could have long term impact in

their behavior and attitude. As it presented in section 2.3.1, there are many sequences caused by the lack of awareness regarding these risks. As a result, there should be a concern on how to educate Libyan secondary school students about these risks, as well as creat a way to aware them about the strategy of defense in any case of presented security risks.

2.3.5: Success of Information Security Awareness

Alhejaili (2013) discussed the usefulness of teaching security awareness for secondary school students, his idea based on providing an online interactive program to reduce risks that could affect the secondary school students. He also stated that there is a need to examine the current state of security awareness among students and their families, and to ensure whether the schools provide an online safety for these students. The finding of this research is based on a quantitative research methodology showed that 94.5% of secondary school students use the Internet and Smartphone and most likely use it for surfing the Internet and social media websites. This study showed that 74.5% of secondary students use the Internet in term of online gaming or online video gaming. This study found that 58.2% of parents did not use the parents filter. The author suggests that "Netismartz" and "OnGuardOnline" are a good educational resource as they provide some information and technical tips on how to deal with some kinds of attack.

Choi et al., (2013) discussed security methods that protect data from unauthorized people to access through physical ways such as eye contacts. They focused on how to apply security awareness programs toward improving security recognition and to contribute the protection of important information.

Olusegun and Ithnin, (2013) applied training to 900 Universiti Technology Malaysia (UTM) students, consisting of staff members to assess their awareness after having information security awareness training (ISAF) program. This program was developed by the group of (ISAF). The finding of this study discovered that ISAF program does not address all the need required by the users. That means there is a need to adjust the program to meet their needs.

Al Omari et al., (2013) investigated the role of ethics in explaining information security policy. To meet the purpose of the study a model that integrates behavioral, ethical and theoretical perspectives was developed and tested. Overall, analyses indicate strong support for the validation of the proposed theoretical model.

Eminagaoglu et al., (2009) in a case study on the positive outcomes of information security awareness training on the biggest transportation enterprise in Turkey. The focused area of this study is the password usage, password quality and compliance of employees with the password policies of the company. The finding of this study showed that the security awareness campaigns have positive impact on the weak password habits among most users, and they have an increase awareness in the way of using and choosing their personal passwords more safely.

SecueInfo (2007) indicated how to be more accurate to assess how information security awareness that the effects on the government posture. This study focused only on federal government workers, and one hundred people were qualified. The study found that the government employees are frequently violating information security policies. A lot of them do not care and follow information security policies and procedures.

Pltler (2005) discussed the successful element of information security awareness program, and he addressed the importance of employees in information security in an organization, and how to make security programs related to the variety of audiences. Pliers' results found that security awareness is a process that needs a perfect change in employees' behaviour. This has to start from the time of employing any employee, and that has to continue with them every year. In addition, security awareness has to start from childhood, and everywhere in different media.

From the statement above it is clear that there must be a research to identify the best tools to apply information security awareness among secondary school students. The expected tools have to be suitable to the age of these students as well as their needs to straighten their security awareness. The tool of measuring of the level of security awareness is another issue that should be focused in this research as it showed in this literature that even the employees still did not have enough awareness on how they have to secure their sensitive information. At this point of view the security awareness has to be started earlier to measure its effectiveness.

2.4: Summary

The literature, studies, and articles discussed in this chapter shown border view on the research area. The overview on the information security awareness help us in getting understanding to the current challenges and weakness that occur in the lack of awareness on this issue. As humans are considered the weakest link in information security, and based on this the current study by this author focused on secondary school students from the perspective of having early knowledge and education will help raise the level of awareness between the chosen samples. The quantitative and qualitative methodology has its advantages in measuring the security awareness as it

concluded from this literature. Moreover, security awareness training program has a great deal in enhancing the security awareness among different participants. Followed the previous researchers, this study employed the same methods as well as a training program.

