CHAPTER III

RESEARCH METHODOLOGY

3.1: Introduction

This chapter intended to define the study method, which is deployed to answer the research questions mentioned in chapter one. Based on the objectives of this study in section 1.4, both quantitative and qualitative methodologies were used for the purpose of collecting and obtaining the data as illustrated in table 3.

Table: 3 Description of Research Activities

PHASE	TASKS
Phase 1	**Literature Review** Definition of the Security Awareness Information Security Risks Security Awareness Training Program Evaluation of Information Security Awareness Information Security Awareness Challenges Success of Information Security Awareness
Phase 2	**Data Collection** Pre-Questionnaire Training Program Post-Questionnaire
Phase 3	**Data Analysis** Reliability Descriptive Analysis Crosstab Mean Anova
Phase 4	**Communicate Results** Research Finding Future Work

3.2: Literature Review

The literature discussed in this research is focused on the related areas such as: security awareness definitions, information security risks, security awareness training program, evaluation of information security awareness, information security awareness challenges, and success of information security awareness. There have been several sources used to obtain the relevant studies such as, Google Scholar, SinceDirect, Elselver, Open Access Library and IEEEXplore Digital Library. Also further searching on relevant publication reports and websites were done to provide a better understanding of the chosen area.

Based on the literature study, it has been observed that few researches considered the age of secondary school students as in our presented security risks "passwords, social networks, cyberbullying". Moreover, there is a less concern on the security awareness training tools that consider secondary school students as well as measure their effectiveness. The methodology of this thesis is based on the findings of the previous literature that evaluated information security awareness.

3.3: Data Collection

This section further discussed the strategy used to fulfil the objectives of this study. The following subsections provide more information about how to apply the research methodology. A survey questionnaire was designed and deployed in order to achieve the purposed reasons in deploying this kind of methodology. An actual training program took place while conducting these questionnaires.

3.3.1: Training Tools

In order to stand on the training tools designed for this age of secondary school students from 13 to 18, a search for the security cyber portals of South East Asia countries as well as the CERTs were conducted. The idea of searching on CERTs and cyber security portals is to get further understanding of the materials offered for educating users with security and how to protect themselves from potential risks. The training materials are organized in its original source, and this based on two cyber portals "Malaysia (Cyber safe)", "Singapore (Cyber wellness)". The tools used in this training are:

- Games
- Videos
- Posters

The aim of these tools is to touch the needs and risks caused by the students, in case if they skip security procedures. All of presented tools contained an explanation on "Passwords, social networks, and cyber-bullying" see appendix C. A briefing about the topics of "Social networks, passwords, and cyber-bullying" were given to the secondary school students in order to provide a deeper understanding of the risks associated with them. Within this training, secondary school students are invited to practice each tools from each cyber portal separately. After students have finished this part, they are required to answer the post questionnaire as in this version the fifth section focused on evaluating the security awareness material that provided from cyber portals from secondary school students' perspective.

3.3.2: Questionnaire Design

The contact with the participants was via paper-based questionnaire. This copy of the questionnaire is contained in the first page a brief statement, details related to the sender of this questionnaire, under which department, and university name. The next parts were a briefing about the meant study, including what are the students required to do, and the expected time on the experiment, and why students should answer this questionnaire.

To assess the level of awareness, pre and post questionnaire conducted. Both pre and post questionnaire are similar. However, there was a significant difference between both of these versions based on the section five in the post-questionnaire. This section was designed especially for evaluating the security awareness training tools that occurred from security cyber portal of South-East Asia. Students are first invited to answer the pre-questionnaire. Upon completion, they were invited to listen and participate in training. After completion of this task, a post-questionnaire were given to them. Both pre and post questionnaire were collected, analyzed and compared to assess their awareness level. While participating in the training, the observation done to observe secondary school students attitude and manner. From this action it is hoped to identify and resolve the qualitative part of the proposed study.

The pre and post questionnaire are the same, and contain four parts, except the fifth part that designed especially for post questionnaire. Each part focuses on specific area see appendix (A, B).

1- The first part: demographics and general security questions.

2- Second part: assessing the security awareness level in terms of social networks, passwords, and cyber-bullying.

3- Third part: assessing security practices of secondary school students on the same security risks of this study.

4- Fourth part: was about secondary school students' personal opinion on security risks of this study.

5- Fifth part: was limited to "section five" focused on evaluating the security awareness training tools based on the secondary school students' practices on the security awareness training program. The questions about this section presented as follows for each country:

- Malaysia Cyber-Safe: games, video, and posters.
- Singapore Cyber- Wellness: games.

3.3.3: Population and Sample

The target group was secondary school students, in the age of 13 to 18 years old. The school of these students was the Libyan secondary school in Malaysia "Kuala Lumpur and Selangor". The sample size was 50 students with mixed gender. These schools are not limited for Libyan students only, as students from other nationalities exists on them. The sample size was under the limitation of time as well as the nature of the study that needs to conduct a training program in the same time with employing the questionnaire.

3.3.4: Steps Students Need to Follow

Students were required to answer the pre questionnaire based on their real practices on everyday life. The students were asked to tick beside every choice that represents their opinion. After this part, students were invited to participate in a security training program based on the chosen security issues. After this training a post-questionnaire was submitted to all the students in order to assess their awareness and practices after the training program. Students are also considered to evaluate the training materials passed on what they understand from these tools.

3.4: Data Analysis

The data analysis gives the meaningfulness of the data collected from the chosen sample. For the purpose of data analysis, SPSS software was used, including Reliability, Descriptive, Crosstab, Mean, and ANOVA.

- **Descriptive Analysis** for all variables by frequency and percentage for each.
- **Reliability Statistics** based on the Cronbach alpha value of the items. The reliability and validity test was carried out at 0.72 for the pre-questionnaire and 0.79 for post –questionnaire according to (George and Mallery, 2003).
- **Crosstab** in order to understand the current awareness level of students in the pre and post-questionnaire.
- **Mean** to provide the highest value of the training materials.
- **ANOVA Statistics** to stand on the relationship and significant level between the variables used in this research.

3.5: Pilot study

A pilot study was carried out in the early time of conducting this study to provide any potential enhancement on the questionnaire. The sample of 10 Libyan secondary school students' pilot tested and the results were used to validate the questionnaire by obtaining the value of Cronbach alpha. The results of the pilot study did not lead to any fundamental changes as it just brought about an enhancement in the design of some questions.

3.6: Consolidation

This section draws the process of conducting this study and the instruments used to obtain the outcome for each task in order to achieve the objectives of this study. The process of this study is as summarized in table 4.

Table: 4 Tasks and Outcome of the Study

Objectives	TASK	OUTCOME
To identify and evaluate available security awareness training tools used for secondary school students	Searching on: ➢ South East Asia cyber portals ➢ CERTs of South East Asia portals	• Available cyber security portals: www.cybersafe.my www.gosafeonline.sg www.cyberwellness.org.sg www.secureverifyconnection.info/svcdev/ http://secudemy.com/ • Available CERTs www.brucert.org.bn/ www.mycert.org.my/en/ www.cert.or.id/beranda/en/ www.phcert.org/ www.singcert.org.sg/ www.thaicert.or.th/about-en.html www.camcert.gov.kh/ www.vncert.gov.vn/en/ www.laocert.gov.la/en/Page-1- www.mmcert.org.mm/ • Available security awareness training materials: ❖ Video ❖ Games ❖ Poster ❖ Newsletters.
To assess the level of security awareness among secondary school students related to social networks, passwords and cyberbullying	➢ Pre-Questionnaire ➢ Training Program ➢ Post-Questionnaire Strategy Used: 1- Reliability Statistics 2- Crosstab 3- Mean 4- ANOVA	• The reliability statistic for all used variables for pre and post questionnaire Training based on the materials provided from South East Asia Cyber portals • The level of awareness for pre and post questionnaire to stand on the usefulness of the training program • The expected tool that will be used to educate secondary school students • Assessing any gender or age differences in the chosen group based on the security awareness and security practices • Observation of students behavior while conducting the training program

3.7: Summary

This chapter describes a detail on the methodology used to achieve the objective of this research. Both quantitative and qualitative methodology were applied in this research. A training program took place based on the cyber portals of South-East Asia. All of the methodology used in this study pilot tested and analyzed to have an overview to the study borders. The data analysis process used SPSS with Reliability statistics, Crosstab, Mean, and ANOVA statistics.