ASSESSMENT OF CYBERSECURITY AWARENESS PROGRAM ON PERSONAL DATA PROTECTION AMONG YOUNGSTERS IN MALAYSIA

NOOR HAYANI ABD RAHIM

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2017

ASSESSMENT OF CYBERSECURITY AWARENESS PROGRAM ON PERSONAL DATA PROTECTION AMONG YOUNGSTERS IN MALAYSIA

NOOR HAYANI ABD RAHIM

THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2017

ABSTRACT

Youngsters aged 12 to 19 years old are among the highest number of Internet users in Malaysia. Characteristically, they have a high degree of enthusiasm. They tend to overshare information, and perceive everything on the Internet as the truth. They also lack security knowledge on how to protect their personal data, do not restrict themselves from sharing it on the Internet. Thus, efforts have been made in Malaysia to educate youngsters regarding the importance of protecting personal data. However, the current cybersecurity awareness module posed few challenges such as on understanding, acceptance of message and effective ways of giving awareness which require an assessment to be conducted. A literature review was thoroughly conducted to justify the lacking elements on assessment of cybersecurity awareness programs, and found that there is little attempt to use program evaluation technique, a lack of focus on youngsters and a lack of assessment on the understanding of personal data protection. Based on the aforementioned limitations, this study aims to identify the assessment criteria's for cybersecurity awareness program based on theories and component of personal data protection, to propose the assessment framework for cybersecurity awareness program, to employ and verify the proposed assessment framework for assessing cybersecurity awareness program among youngsters. This study used a mixed method research design, where the data collections were conducted over four distinct in sequential phases. In Phase 1, a survey of 384 youngsters was conducted. In Phase 2, a pre-test and post-test survey was conducted on 397 and 391 youngsters respectively. In Phase 3, three focus group interviews were conducted. Finally, in Phase 4, observation of web recording was conducted using Camtasia Studio to record the youngsters' online activities. Phase 3 and 4 were made up of 12 youngsters divided into 3 focus groups. All were held at two OUTREACH CyberSAFE programs conducted by Cybersecurity

Malaysia. Firstly, at Bahagian Teknologi Pendidikan Negeri Johor which involved youngsters from all over Malaysia, and secondly at Sekolah Seri Puteri Kuala Lumpur. Analyses were done using SPSS and thematic analysis. The findings show that the current module has a positive degree of favourability in terms of the youngsters' reaction and raised their knowledge and skills on personal data protection. Besides, this study also proposed four effective ways to enhance the current module of cybersecurity awareness. This includes the element of decision making in using personal data, the management of online applications, online content, usernames and passwords. From the theoretical contributions perspective, this study identified assessment criteria's based on ARCS Model of Motivational Design Theory, SLT and TRA that used to nominate Kirkpatrick's Four Learning Evaluation Model that used as the assessment guideline. From the practical contribution perspective, this study facilitates stakeholders such as Cybersecurity Malaysia, parents and school management to decide for a better module to convey the message on personal data protection.

ABSTRAK

Golongan muda berumur 12 hingga 19 tahun adalah antara pengguna Internet tertinggi di Malaysia. Secara lumrahnya, mereka mempunyai semangat tinggi dan cenderung untuk menyebarkan maklumat, dan menganggap semua yang dipaparkan di Internet adalah benar. Mereka juga kekurangan pengetahuan keselamatan dalam melindungi data peribadi dan tidak mengambil pendekatan untuk menyekat perkongsian data peribadi di Internet. Oleh itu, usaha telah dibuat di Malaysia untuk mendidik golongan muda tentang kepentingan untuk melindungi data peribadi. Walau bagaimanapun, modul kesedaran keselamatan siber yang sedang digunakan memerlukan penilaian kerana beberapa cabaran seperti keberkesanan tahap pemahaman, penerimaan dan kandungan mesej serta cara-cara berkesan untuk memberi kesedaran. Kajian literatur secara teliti telah dijalankan untuk membuktikan unsur-unsur kekurangan di dalam penyelidikan sebelumnya mengenai penilaian program kesedaran keselamatan siber. Kami mendapati bahawa teknik penilaian program tidak digunakan, kurang tumpuan diberikan kepada golongan muda dan kekurangan penilaian tentang perlindungan data peribadi. Berdasarkan unsur-unsur kekurangan yang dinyatakan di atas, kajian ini bertujuan: i) mengenalpasti kriteria penilaian untuk program kesedaran siber berdasarkan teori dan komponen perlindungan data peribadi, ii) mencadangkan rangka kerja penilaian untuk program kesedaran siber, iii) mengguna dan mengesahkan kerangka penilaian dan akhir sekali membuat pengesahan tentang penggunaan kerangka penilaian untuk program kesedaran siber di kalangan remaja. Kajian ini menggunakan reka bentuk penyelidikan kaedah campuran, di mana pengumpulan data dilakukan di dalam empat fasa secara berturut-turut. Dalam Fasa 1, tinjauan terhadap 384 golongan muda telah dijalankan. Dalam Fasa 2, satu kajian pra-ujian dan ujian pasca ujian masing-masing dijalankan terhadap 397 dan 391 golongan muda. Dalam Fasa 3, tiga temu bual kumpulan fokus dijalankan. Akhirnya, dalam Fasa 4, pemerhatian rakaman

web dilakukan menggunakan aplikasi Camtasia Studio untuk merakam aktiviti golongan muda di dalam talian. Bagi Fasa 3 dan 4, 12 golongan muda dibahagikan kepada 3 kumpulan fokus. Pengumpulan data telah diadakan di dua program OUTREACH CyberSAFE dijalankan oleh Cybersecurity Malaysia. Pertama, bertempat di Bahagian Teknologi Pendidikan Negeri Johor yang melibatkan golongan muda dari seluruh Malaysia, dan yang kedua di Sekolah Seri Puteri Kuala Lumpur yang hanya melibatkan golongan muda yang berlajar di sekolah ini. Analisis telah dijalankan dengan menggunakan SPSS, dan analisis tematik. Penemuan menunjukkan bahawa modul semasa mempunyai tahap kesukaan yang positif dari segi reaksi golongan dan meningkatkan pengetahuan dan kemahiran mereka terhadap perlindungan data peribadi. Selain itu, kajian ini juga mencadangkan empat cara yang berkesan untuk meningkatkan modul kesedaran keselamatan siber. Ini termasuklah elemen membuat keputusan dalam menggunakan data peribadi, pengurusan aplikasi dalam talian, kandungan dalam talian, nama pengguna dan kata laluan. Dari perspektif sumbangan kepada teori, kajian ini telah mengenalpasti kriteria penilaian berdasarkan Model ARCS Teori Reka Cipta Motivasi, SLT dan TRA yang digunakan untuk mencalonkan Model Penilaian Pembelajaran Empat Kirkpatrick yang digunakan sebagai panduan utama dalam kerangka penilaian. Dari perspektif sumbangan praktikal, kajian ini memudahkan para pihak berkepentingan seperti Cybersecurity Malaysia, ibu bapa dan pengurusan sekolah untuk memutuskan modul yang lebih baik untuk menyampaikan mesej mengenai perlindungan data peribadi.

ACKNOWLEDGEMENTS

Assalamualaikum and all my praise to Allah SWT for granted me with health, spirit and motivation to complete this journey. Alhamdulillah with all the blessings, I managed to complete this thesis as part of my doctoral program at University of Malaya. My first acknowledgement is to my sponsorship, Ministry of Higher Education Malaysia and International Islamic University Malaysia. To my advisor Dr. Suraya Hamid and Prof. Dr. Miss Laiha Mat Kiah, their support and guidance is priceless. I am very grateful for their attention, courage, inspiration and endless coaching. I especially thank University of Malaya and Cybersecurity Malaysia for providing me with the great environment and facilities in assisting my research. Not to forget all participants involve in this research. My thanks also go to the faculty members and colleagues. Without them I would not come this far. For Hani Syazilah, Ely Salwana and Suraya Ika. We shared ideas, laugh and sad moment together. My journey is incomplete without all of you.

My next acknowledgement is for my late father Hj. Abd Rahim Bahaudin and mother Hjh. Noor Ainee Hj. Ebau. Thanks for your love, prayers, motivations, constant support and strength for my progress. I also would like to express my gratitude to my mother and father in laws, Abdul Hamid Jaafar and Rahimah Karim and all my families for their prayers and courage.

Finally, I owe great amount of gratitude for my husband Abdul Rahim Abdul Hamid. He lived with me through the journey and always supports me with his loves and words to make me stronger and stay calm. To my daughters Hannah Safiyyah, Haneen Medina and son Muhammad Hadif Mukhlis I always found my relaxation and calmness from their pure smile and laugh. I solely dedicate this thesis for them.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ARCS	ARCS Model of Motivational Design Theory
BTPN	Bahagian Teknologi Pendidikan Negeri
CIPP	Context, Input, Process, Product
CSM	Cybersecurity Malaysia
CyberSAFE	Cybersecurity Awareness for Everyone
IT	Information Technology
IS	Information System
MCMC	Malaysian Information Technology Council
MOSTI	Ministry of Science, Technology and Innovation Malaysia
NISER	National ICT Security and Emergency Response Centre
NITC	National Information Technology Council
PB	Program Benefit
PC	Program Content
PPC	Program Presentation and Component
SLR	Systematic Literature Review
SPSS	Statistical Software Package for Social Science
SLT	Situated Learning Theory
RQ	Research Question
ROI	Return on Investment
RO	Research Objective
TRA	Theory of Reasoned Action

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION AND RESEARCH BACKGROUND

Concerns regarding cybersecurity breaches has urged for the need of confidential information and storage media protection from being compromised (Dlamini, Eloff, & Eloff, 2009). The protection methods used should be continuously updated and enhanced in line with new technological developments to counter the increasingly sophisticated threats to cybersecurity which are originated from unforeseen sources on the Internet (Choo, 2011; Dlamini et al., 2009). The nature of cyber threats today are more dynamic, sophisticated, complex and unprecedented in terms of scope, skill, frequency, capacity and capability in targeting victims. This has resulted in serious financial loss (Lewis, 2014; Albrechtsen, 2007).

The main factor contributing to change in cyber threats is the increasing global population in using the Internet (Meekin, 2016; Saran, 2016; Choo, 2011). As of June 2014, it has been reported that over three billion people worldwide are using the Internet, in which the percentage of Internet users are Asia (49.5%) Europe (17.2%), Latin America/Caribbean (10.5%) and the remaining are from Africa, North America, Middle East and Oceania/Australia (ITU, 2014; Internet World Statistics, 2014). There have been uptrend surges in the usage of internet due to new applications. The recent development of the Internet has encouraged people to explore its technology in various applications such as virtual broadcasting, Internet of things, information sharing, online banking, shopping as well as both interactive communication and socializing via social media as mentioned by

Gubbi, Buyya, Marusic, & Palaniswami (2013), Lenhart, Purcell, Smith, & Zickhur (2010) and Leiner et al.(1997). This development has prompted many parties and groups to join the Internet community.

Internet communities differ and most often, the reported users are youngsters ranging from 12 to 19 years old. Youngsters are frequently categorized as the most active Internet users, as they are surrounded by smart devices such as smartphones. It enables them to connect to the Internet at any time (Amanda Lenhart, 2015; Madden, Lenhart, Duggan, Cortesi, & Grasser, 2013; Atkinson, Furnell, & Phippen, 2009). This statement is supported by a study of more than 2000 American households based on the number of Internet users by age, which revealed that since 2000 till 2012, youngsters constituted the highest percentage and most active Internet users (Cole, Suman, Schramm, Zhou, & Salvador, 2013). Supported by recent data from Pew Internet Research Group, youngsters compared to the elderly, are more active with online shopping, spend more time online, more exposed to media content and valued social networking sites as a way to maintain and create new relationships (Cole et al., 2013; Madden et al., 2013). Thus, the wide use of Internet applications can expose youngsters to a wide range of cyber threats. This is because cybercriminals exploit technology to reach to Internet users, especially youngsters, and launch various means of online attacks (Atkinson et al., 2009). This includes the risk of silent invasion of individual privacy that is specifically targeted in obtaining individuals' personal data for illegal means (Broadhurst & Chang, 2012; Aimeur & Schonfeld, 2011; Loibl, 2005).

Throughout this thesis, the following three terms are frequently used: While these terms are closely related, there are some differences (i) "Cybersecurity" – referring to the

organization and collection of resources, processes, and structures which is normally used to protect cyberspace and cyberspace-enabled systems from any occurrences against property rights (Craigen, Diakun-Thibault, & Purse, 2014), (ii) "Cybersecurity awareness program" – is briefly defined as a methodology to educate Internet users to be sensitive to various cyber threats and the vulnerability of computers and data to these threats (Siponen, 2000), (iii) "Cyber threats" – referring to the act of violence using the Internet as medium or other information communication technologies (Willard, 2006).

In coping with the cyber threat landscape that has shifted from the use of savvy hacking skills to sophisticated and well-planned strategies, cybersecurity awareness is deemed essential for Internet users like youngsters as a counter-measure to combat silent privacy invasions (Choo, 2011; Dlamini et al., 2009; Furnell, Tsaganidi, & Phippen, 2008). It also served as the right platform to instil security culture in personal data protection. The message of cybersecurity awareness must be effective and should address all ages, encompassing both the workplace and domestic environments. It is also important to ensure that the message of cybersecurity is well-conveyed and all relevant audiences receive adequate attention. Based on the literature of cybersecurity awareness program, it has brought urgent attentions by many researchers to introduce and educate via by various methods such as classroom-based, training, programming as well as applications (Ashenden, 2015; Allam, Flowerday, & Flowerday, 2014; Arachchilage & Love, 2014; Chen, Shaw & Yang, 2006; Furnell, 2008; Rezgui & Marks, 2008). The intention of Cybersecurity awareness is to scare or create apprehension among Internet users but instead to equip and prepare users for a contingency plan against cyberattacks. It is also an appropriate platform to disseminate information concerning new cybersecurity threats

(Choo, 2011). Users' knowledge of cybersecurity is important to cope with emerging Internet technologies which are associated with an increased speed and greater sophistication of cyberattacks (Ciampa, 2013). It is also important to increase knowledge on cybersecurity due to changes in users' behaviour, and the wide use of online services such as banking, social networking, cloud computing, Internet of things and information economy which has promoted the widespread practice of distance communication (von Solms & van Niekerk, 2013; Whitson, 2009; Thomson & Solms, 1998). It is important for the message to be conveyed through a cybersecurity awareness program to be clearly presented and be easily understood. The focus should be stressed on specific individual factors such as age, gender and educational level. Furthermore, the message delivered should be accurate and concise by providing real-life examples and by using the right delivery methods (Farooq, Isoaho, Virtanen, & Isoaho, 2015; May, 2008). A cybersecurity awareness program shall be an on-going initiative that requires continuous effort to educate and update Internet users of cyber threats (Abawajy, 2014; Tsohou, Karyda, Kokolakis & Kiountouzis, 2014 Kruger, Drevin & Steyn, 2006).

A cybersecurity awareness program normally followed by an assessment (Abawajy, 2014; Abawajy, Thatcher, & Kim, 2008). The purpose of this assessment varies but mainly regarding on capturing participant's feedback, their level of understanding and security culture practiced. There are various ways to conduct assessment such as using survey, game tools and interview (Rahim, Hamid, Mat Kiah, Shamshirband, & Furnell, 2015). However, thus the current assessment really works in capturing feedback from youngsters require further investigation on the current approaches of cybersecurity awareness program assessment. This is because youngsters differ in term of their acceptance, understanding of

the security concept and promoting a security culture (Ciampa, 2013; Rantos, Fysarakis, & Manifavas, 2012 Knapp & Ferrante, 2012; Kruger et al., 2006; Kruger & Kearney, 2006). One of the contributing factor is the behaviour of youngsters, their overly enhance confidence in using their personal computers and mobile devices which can lead to reluctance in embracing security measures (Furnell, 2008). In addition, the lackadaisical attitude towards security causing youngsters to be the weakest link in the security chain (Fahrnberger, 2014; Warren & Streeter, 2013; Gross & Rosson, 2007). They are also often ignorant and naive on security issues (Richet, 2015; Pramod & Raman, 2014; Furnell & Thomson, 2009). Thus the assessment shall be focused and comprehensive to ensure good input derived in the process of enhancing the quality of cybersecurity awareness program. Considering the issues discussed with regard to youngsters and concern over their personal information, it is important for the assessment to focus on youngsters and personal data protection at the same time. Besides, the approach taken to identify assessment criteria's is also important. Therefore, this study aim to propose assessment framework that are based on the theories and components of personal data protection and employ it in conducting an assessment among youngsters. Thus, it is justify for the consideration to focus on the assessment of cybersecurity awareness program among youngsters particularly on personal data protection. The following section outlines the problem of previous cybersecurity awareness program assessment approaches in term of methodology used. This is to determine whether or not youngsters are considered as part of the target unit of analysis for the assessment and whether personal data protection is considered part of the assessment.

1.2 PROBLEM STATEMENT

The investigation on the assessment approaches for cybersecurity awareness programs revealed a lack of attempt to conduct the assessment based on program evaluation model. The program evaluation model addressed here is an evaluation method and technique which involves a systematic and dynamic procedure for performing evaluation, judgment, investigation, decision making, improvement, upgrading and assessment of any social intervention program (Yarbrough, Shulha, Hopson, & Caruthers, 2011; Rossi, Lipsey, & Freeman, 2004; Royse, Thyer, Padgett, & Logan, 2001). In a study done by Abawajy et al., (2008) on the assessment of human factors, they suggested that the use of program evaluation model namely Kirkpatrick's Four Learning Evaluation Model (reaction, learning, behaviour and result) to evaluate the effectiveness of the cybersecurity awareness program. However, previous literature showed that the actual use of this technique is less considered and is not justified as assessment criteria for an assessment of cybersecurity awareness programs. In addition, most of the current assessment criteria merely for determining the general experience and usage of security measures, the attitude while accessing the Internet, and security perception (Furnell et al., 2008; Furnell, Bryant, & Phippen, 2007). In the study conducted by Al-Hamdani (2006), the assessment was made on the following criteria: information security in general, and understanding of a few topics concerning security. Other studies were focused solely on the user behaviour without looking at other criteria of assessment (Ng, Kankanhalli, & Xu, 2009; Stanton, Stam, Mastrangelo, & Jolton, 2005). Therefore, this study attempts to fill in the gaps in assessment of cybersecurity awareness research by identifying assessment criteria's that can be mapped to select the appropriate program evaluation model.

Further investigation upon literature on the assessment of cybersecurity awareness programs also revealed that the focus groups mainly targeted for assessment were organizations and home Internet users (Furnell, 2010; Gross & Rosson, 2007; Kruger & Kearney, 2006). It seems that the scope of these two contexts is too broad and requires proper segmentation during assessment due to the fact that Internet communities varies and possess different understanding and unequal level of security awareness among different age groups (Shaw et al., 2009; Abawajy et al., 2008). There were attempts made by Furnell et al. (2007) and Furnell et al. (2008) to assess the security perception and find the security belief of personal Internet users. However, the study randomly focused on general Internet users without segregation in terms of age segmentation, especially with youngsters. Thus, the need for assessment according to age segmentation is warranted and this study attempted to fill this gap by focusing the assessment on youngsters as respondents and participants.

The extended investigation on the assessment of cybersecurity awareness programs in relation to the increase in identity theft among youngsters revealed that they were found to have a lack of understanding, and poor security behaviour with regards to personal data protection. As an example, to make sure they are safe from being visible to the public while accessing the Internet (Shaw et al., 2009; Furnell et al., 2008). Also in an analysis done by Talib, Clarke, & Furnell (2010), it was discovered that personal data such as real names, email addresses, real dates of birth and full addresses were made available on the Internet. This can facilitate identity thieves to capture this information and use it for illegal means (Aimeur & Schonfeld, 2011). Youngsters can easily become a victim due to their ill equipped nature with regards to the practice of Internet safety (Furnell, 2010). Based on the

literature, it was found that most of the assessment of cybersecurity awareness sessions available was generally focused on a broad security concern but with less focus specifically on creating awareness on personal data protection. Therefore, this study attempted to fill this gap by focusing particularly on the assessment of personal data protection among youngsters.

To recap the direction of this thesis, this study attempted to conduct assessment of cybersecurity awareness program on personal data protection among youngsters. The output of this study is in the form of identified assessment criteria's used as proposed conceptual framework and employed in assessing youngsters. The propose conceptual model is beneficial to facilitate stakeholders such as Cybersecurity Malaysia, parents and school management to gain youngsters feedback and further decide the best module to convey cybersecurity awareness program on personal data protection.

1.3 RESEARCH OBJECTIVES

Based on the problems mentioned in the previous section, the following are the research objectives (RO). This study was formulated to reach the following objectives.

RO1. To identify the assessment criteria's for cybersecurity awareness program based on theories and components of personal data protection.

RO2. To propose an assessment framework for cybersecurity awareness program.

RO3. To employ the proposed assessment framework for assessing cybersecurity awareness program among youngsters.

RO4: To verify the proposed assessment framework for cybersecurity awareness program.

1.4 RESEARCH QUESTIONS

There are three primary research questions formulated in this study. They were mainly developed for making an assessment on the current cybersecurity awareness module. The following are research questions (RQ) for each research objective (RO) outlined in more specific terms:

RQ1. What are the identified assessment criteria's for cybersecurity awareness program based on theories and components of personal data protection?

RO1. To identify the assessment criteria's for cybersecurity awareness program based on theories and component of personal data protection.

RQ2.What is the proposed assessment framework for cybersecurity awareness program?

RO2. To propose an assessment framework for cybersecurity awareness program

RQ3.How to employ the proposed framework for assessing cybersecurity awareness program among youngsters?

RO3. To employ the proposed assessment framework for assessing cybersecurity awareness program among youngsters.

RO4: To verify the proposed assessment framework for cybersecurity awareness program.

In summary, the first research questions (RQ1) focuses on the identification of assessment criteria's based on selected theories and components of personal data protection. The second research questions (RQ2), focusses on connecting the identified assessment criteria's in the form of framework for actual assessment conducted in (RQ3). Verification with panel experts is performed in order to answer (RQ3).The mapping of research questions with its corresponding research objectives, methods and activities, deliverables and corresponding chapters is presented as the following Table 1.1 .

Table 1.1: Mapping of Research Gap and its Corresponding Research Objectives and Research Questions

Research questions	Research objectives	Method and activities	Deliverables	Corrrespondin g chapters
RQ1. What are the identified assessment criteria's for cybersecurity awareness program based on theories and components of personal data protection?	RO1. To identify the assessment criteria's for cybersecurity awareness program based on theories and components of personal data protection.	1) Literature review on the components of personal data protection 2) Literature review on selected theories regarding individual assessment criteria's 3) Literature review on the program evaluation model 4) Initial list of identified assessment criteria's from the theory	1) List of assessment criteria's based on components of personal data protection 2) List of assessment criteria's based on theories 3) List of identified assessment criteria's for cybersecurity awareness program	2 & 3
RQ2. What is the proposed assessment framework for cybersecurity awareness program?	RO2. To propose an assessment framework for cybersecurity awareness program	1) Mapping the initial list of identified assessment criteria's from the theories with appropriate program evaluation model 2) Incorporate the component of personal data into the identified assessment criteria's 3) Draw logical diagram to connect the identified assessment criteria's (RO1) based on selected program evaluation model and component of personal data protection	1) Proposed conceptual framework	2 & 3
RQ3. How to employ the proposed framework for assessing cybersecurity awareness program among youngsters?	RO3(a). To employ the proposed assessment framework for assessing cybersecurity awareness program among youngsters. RO3(b): To verify the proposed assessment framework for cybersecurity awareness program.	1) Identify suitable research methodologies 2) Developed instruments based on proposed framework 3) Conduct Content – Related Validity by Expert Panel (C-RVEP) for each developed instruments. 4) Post C-RVEP - Modification of instruments. 5) Conduct pilot study. 6) Post pilot study - Modification of instruments. 7) Conduct actual data collection. 8) Perform data analysis 9) Integrate assessment result. 10) Used the integrated assessment result to identify focused content on personal data protection. 11) Used the integrated assessment result to identify emerged findings 12) Verify the findings with Panel Expert.	1) Identified methodologies 2) Set of developed instruments 3) Assessment result for each instrument used. 4) Integration of assessment result from different methodologies used. 5) Identified focused content on personal data protection 6) Identified emerged findings. 7) Verified framework.	4 & 5

1.5 RESEARCH SCOPE

In order to achieve the RO of this study and to employ the assessment of cybersecurity awareness program among youngsters, this study leveraged on Cybersecurity Malaysia (CSM), an organization that is responsible to provide response, management as well as education to various types of online security incidents.

In addition to that, the scope of this study was limited to the cybersecurity awareness program conducted by Cybersecurity of Malaysia. It does not involve any other cybersecurity awareness programs conducted by other organizations nationally or internationally. The selected participants for this study are youngsters ranging from 12-19 years old. The youngsters incorporated in this study attended the cybersecurity awareness program conducted by Cybersecurity Malaysia. The instrument for this study was designed towards analysing the feedback and information pertaining to personal data protection only.

Data was collected and analysed based on the proposed conceptual framework as in section 3.10 by means of surveys, pre-test and post-test survey, focus group interviews and observation of web recordings.

1.6 RESEARCH DESIGN

A research design is defined as a methodological scheme to adhere in order to attain the identified research objectives and to answer the research questions. This study uses research design proposed by Lewis (1998), outlined in Figure 1.1 together with activities taken and its corresponding RO, while the details are discussed in Chapter 4. There are four main steps namely analysis, design, development and evaluation. The analysis step is theoretical in nature, involves literature search on the current approaches to conduct assessment of cybersecurity awareness program, concern over youngsters and personal data protection, the identification of assessments criteria's based on theories, program evaluation model and component of personal data protection.

The next step is design, where the deliverable from the analysis step is translated into proposed conceptual framework for assessing cybersecurity awareness program. The design step also translates the proposed conceptual framework into actual instruments to be used during the development step. The next step is development; it is aimed at using and testing the proposed conceptual framework by conducting the empirical assessment among youngsters. This step is to ensure the proposed framework works and able to produce useful assessment result.

Finally, the fourth step is evaluation aimed at verifying and validating the result of the research with panel expert with regard to the usefulness of proposed conceptual framework and emerged findings from the assessment result.

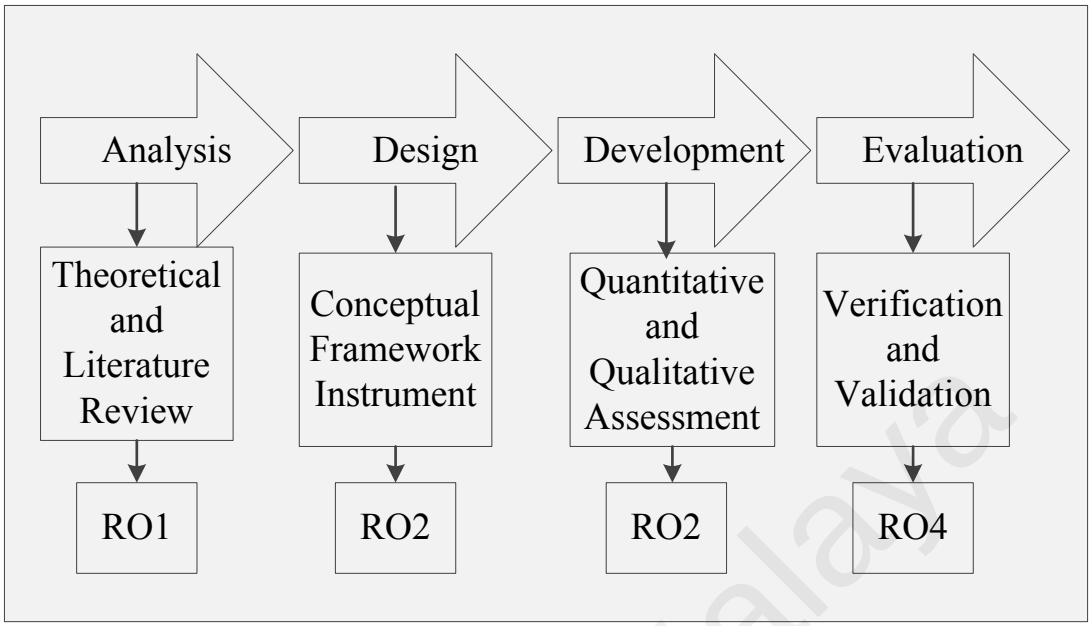

Figure 1.1: Research Design (Adopted from Lewis, 1998)

1.7 RESEARCH CONTRIBUTIONS

The result from this study is vital in understanding the suitable assessment criteria's for assessing cybersecurity awareness program and in discovering the youngsters understanding and feedback regarding personal data protection. This study also propose and use framework for assessing cybersecurity awareness program which could be used by stakeholders such as Cybersecurity Malaysia, authorized organization that conducts cybersecurity awareness program as well as school management and parents. This will assist them to have better decision and planning of conducting future cybersecurity awareness program involving youngsters.

From a theoretical point of view, this study employs the assessment criteria's from Attention, Relevance, Confidence and Satisfaction Model of Motivational Design Theory (Keller & Kopp, 1987), Situated Learning Theory (Lave, & Wenger, 1991) and Theory of

Reason Action (Ajzen, 1985) in proposing the assessment framework for cybersecurity awareness program. When all combined assessment criteria's found in the theories were applied in assessment of cybersecurity awareness program, they provide some useful insight into the current assessment practice This study contributes to enriching the utility of Attention, Relevance, Confidence and Satisfaction Model of Motivational Design Theory (ARCS), Situated Learning Theory (SLT) and Theory of Reason Action (TRA) in proposing assessment framework for cybersecurity awareness program particularly conducted among youngsters. Besides, the mapping made between the identified assessment criteria's from ARCS, SLT and TRA with Kirkpatrick Four Learning Evaluation Model has extended the usage of theory in proposing quality assessment framework which has not been applied before.

Secondly, in terms of practicality, this study proposes a framework to assess cybersecurity awareness programs. This study also assists to improve the methodology in finding suitable content on personal data protection gained through empirical assessment conducted among youngsters for consideration in conducting future cybersecurity awareness program. Besides, this study also promotes experience of conducting evidence-based research which is based on real life experience and evidence among youngsters. Furthermore, it is also beneficial in facilitating stakeholders to decide or plan a better module to convey the message on personal data protection to youngsters. The best module can assist in educating youngsters which can result in decreasing the number of security fraud cases that involve stolen personal data.

1.8 THESIS ORGANISATION

This thesis is organized into six chapters:

Chapter 1 discusses the basic element of this research through brief introduction and research background. This chapter also introduce the problem statement regarding the current assessment approach on cybersecurity program. The elements that are lacking were highlighted and strategy to tackle this problem has outlined in research objective, research questions and subsequently research design. The research contributions in term of theoretical and practical also highlighted in this chapter.

Chapter 2 reviews the literature in relation to the trend of internet usage among youngsters, concern over their personal data protection approaches and cybersecurity awareness program. The thorough review was made to the previous approaches to assess cybersecurity awareness program and its problems is recognized. This chapter also review the components of personal data protection used to assess cybersecurity awareness, and identifies research problems. This chapter also reviews all the relevant theories in order to find the assessment criteria's. This chapter also review literature with regard to program evaluation model and components of personal data protection.

Chapter 3 provides theoretical foundations and proposal for conceptual framework. Theories were reviewed in this chapter and derived to identify assessment criteria's. The identified assessment criteria's is use to select the appropriate program evaluation model to be used as proposed conceptual framework.

Chapter 4 explains the research methodology used throughout this study. This chapter encompasses the selection of the research paradigm, sample selection, construction of instrument and data collection procedure.

Chapter 5 describes the steps taken for data analysis and presents it significant result. It also explain the integration of assessment result and its emerged findings.

Chapter 6 presents the main discussion drawn from the data analysis and shows the answer to the formulated research questions. It also revisits the proposed conceptual framework and shows how the conceptual model had been used. This chapter also discusses research contributions to theory and practice. The recommendation, limitation, implication, conclusion and suggestion for future work are also presented in this chapter.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter aims to establish a review of existing research on the assessment of cybersecurity programs and its related topics. This chapter starts by discussing related research background which involves the trend of Internet usage in Malaysia, the trend of Internet usage among youngsters and their characteristics while using the Internet. Followed by a general overview on cybersecurity awareness in terms of its definition and importance, reliable body that conducts security awareness in Malaysia, together with its content, target audience and delivery approach. This chapter continues on with explaining personal data protection issues with regard to Internet among youngsters. The final section of this chapter presents the core findings of the literature review which warrants a study on the assessment of cybersecurity awareness programs among youngsters. The methodology, targets audience and scope of assessment are also thoroughly discussed.

2.1.1 The trend of Internet usage in Malaysia

According to Leiner et al. (1997), the Internet was first introduced in 1962. However, it took years for the Internet to be introduced to the Malaysian community. According to APNIC (2004), the Internet was first introduced to Malaysia back in 1992 as a government effort to bring the Malaysian community ahead in terms of information processing and to experience advanced technology. Until 2012, based on the Malaysian Communication and

Multimedia Commision, (2013) it was revealed that approximately 18.6 million of the Malaysian population, regardless of location, have access to the Internet. The rapid growth is shown in the statistics made by the Internet World Stats, as of June 2014, the number of Internet users in Malaysia has increased up to 20 million. The statistic has shown significant growth. The rapid growth of the Internet in Malaysia is part of an effort to transform the Malaysian economy from agriculture based to industrial based which requires Internet usage as the backbone for effective communication. The trend of Internet usage in Malaysia involves different demographic backgrounds. This includes different ethnics, gender, age groups, purposes and income. It was also revealed through the Internet User Survey made by the Malaysian Communication and Multimedia Commision (2014) as shown in (refer to Figure 2.1), that youngsters below 19 years old are among the highest Internet users recorded (refer to Figure 2.1). Youngsters, recorded at 15.5%, are the third highest Internet user in Malaysia after 20-24 years old and 25-29 years old categories. This number has shown a significant involvement of youngsters in the Internet usage.

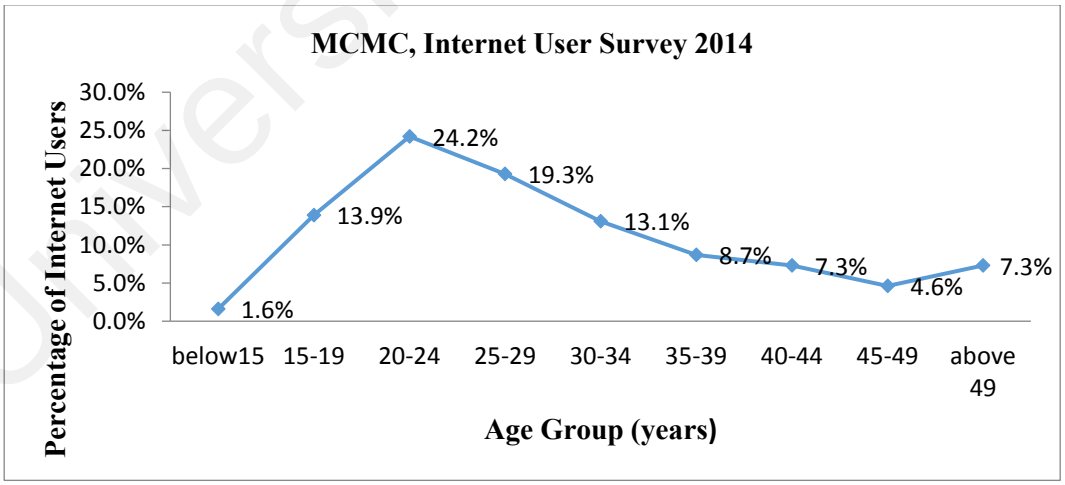

Figure 2.1: Malaysian Communications and Multimedia Commission Internet User Survey 2014

2.1.2 The trend of Internet usage among youngsters

The Internet has inevitably affected the youngsters' daily activities. As early adopters, youngsters are more exposed to Internet exploration and using new technologies inclusive of the Internet (Micheli, 2015; Correa, Straubhaar, Chen, & Spence, 2013; Sieber & Sabatie, 2003). Youngsters or millennials are categorised as individuals aged ranging between 12 and 19 years old (Atkinson et al., 2009; Livingstone, Bober, & Helsper, 2005; Johansson & Götestam, 2004). Often labelled with term NetGen, youngsters who were born surrounded by Internet technologies and smart devices are among the most active Internet users (Johnson, 2006; Oblinger, & Oblinger, 2005). They are highly involved with social media and Internet applications such as YouTube, WeChat, WhatsApp and various gaming applications. Youngsters during the early days use Internet mainly for education purpose with the main focus to promote multimedia content for an interactive learning (Halal, & Liebowitz, 1994). Progressing to 1995, when the Information Technology literacy increased and Internet become as a necessity component in life, the issue of appropriate use of the Internet at home and in schools has been raised and escalated worldwide (Mhlaba, 1995). Scholarly discussion with regard to youngsters, computers and their Internet usage has generally started involving the educational benefits of home computers for children (Schall, Patricia, & Skeele, 1995). However, as the Internet grows and introduction of social media has encouraged youngsters to browse social media sites and it is becoming the most common activity of today's youngsters. Among the most common online social media site, involving social networking such as Facebook, MySpace, and Twitter; gaming sites such as Crytex and Shogun 2: Total War and video sites such as YouTube (O'Keeffe, Clarke-Pearson and Council on Communications and Media, 2011;

Sieber & Sabatie, 2003). Nowadays, the usage of the Internet among youngsters is not only limited to education, but is more focused on social interaction (Ólafsson, Livingstone, & Haddon, 2013; Smahel et al., 2012).

Youngsters these days are fully equipped with gadgets like mobile telephony and smartphones which enable them to acquire Internet access. This is one of the main factors for youngsters to have high involvement in Internet usage (Correa et al., 2013; Madden et al., 2013; Amanda Lenhart et al., 2010). Youngsters normally use the Internet for social media opportunities as well as entertainment, which is mostly done via the use of smartphones and computer tablets (Micheli, 2015; Madden et al., 2013). Youngsters in particular, have unique characteristics in browsing the Internet due to their attitude that is keen to explore and discover new things (Ramli, Hassan, Osman, Shaffril, & Azril, 2014; Vandoninck, D'Haenens, & Smahel, 2014; Livingstone et al., 2005). They also have a high degree of enthusiasm and belief in whatever information available on the Internet is considered genuine and trustworthy. To a certain degree, youngsters sometimes overshare their personal data over the Internet. Using social media for instance, youngsters who share their personal information on the Internet will open doors for threats and making them vulnerable. Due to this attitude, they are becoming so vulnerable in the cyber environment and become an easy target for cyber criminals to take advantage over them. Therefore, it is required to educate youngsters on personal data protection as their extensive use of the Internet may cause harms by attracting the cyber criminals.

2.1.3 The characteristics of youngsters while using the Internet

The consistent finding of high Internet literacy among youngsters as compared to studies in elderly (Kok, Ng, & Kim, 2010; Livingstone et al., 2005), is another reason that justified the need of this study to focus on youngsters to ensure that they gain the appropriate security awareness. Their enthusiasm in exploring the Internet often exposes them to risks of cyber threats, such as phishing and identity theft (Vandoninck et al., 2014; Furnell, 2010). Other reason for conducting assessments among youngsters is the lack of awareness of safety measures, security practices, and reliability of Internet applications (Furnell, 2010; Livingstone et al., 2005). In addition, youngsters have an oversharing attitude on online media, thus encouraging third parties or intruders to stalk or steal personal information. Further investigation on youngsters reveals that popularity, or becoming famous in the digital world, has also encouraged youngsters to get connected to the Internet. They usually upload videos, profile or materials which attract other Internet users to view and share (Micheli, 2015; Sithira & Nguwi, 2014; Lenhart et al., 2011; Lenhart et al., 2010). At a young age, youngsters are often lack in self-monitoring skills, and have difficulty filtering unpleasant online material such as sexual content and misleading communication (Vandoninck et al., 2014). Because of these characteristics, the digital environment is an unsafe medium for them, especially in terms of their personal data. Thus cybersecurity awareness is considered an appropriate platform to educate and keep reminding them of the risk and danger of using the Internet.

2.2 CYBERSECURITY AWARENESS PROGRAM

A cybersecurity awareness program is defined as a way to educate and increase alertness about computer threats and vulnerabilities with regard to IT usage (Siponen, 2000). Another purpose of this program is to increase the level of understanding about self-responsibility and the necessary actions required while engaging in digital activities. Various methods can be used to promote cybersecurity awareness regardless of the age of the individual, for example, classroom-based training sessions, educational videos, seminars, workshops, pamphlet distribution, online advertisement, and e-learning (Da Veiga, 2015; Farooq et al., 2015; Abawajy, 2014; Talib et al., 2010). A cybersecurity awareness program should be conducted frequently to remind and update Internet users regarding the new potential Internet threats (Da Veiga, 2015; Kruger & Kearney, 2006). In Malaysia, an agency has been established as a reliable organisation to conduct and manage cybersecurity awareness among Malaysia citizens. The agency is known as Cybersecurity Malaysia.

2.2.1 Cybersecurity Malaysia

Cybersecurity Malaysia (CSM) was established in 1997 to promote awareness to the Malaysian community, by using MyCert as a division name. It was one of the divisions under MIMOS Berhad. MIMOS Berhad is an agency established under the Ministry of Science, Technology and Innovation Malaysia (MOSTI). It is responsible to serve as a central role in providing technology for information and communications, industrial electronics and nano-semiconductors. In 1998, due to emerging usage of Internet

technology in Malaysia, the National Information Technology Council (NITC) proposed the establishment of the National ICT Security & Emergency Response Centre (NISER). NISER was created as a department under MIMOS Berhad. This resulted in the placement of MyCERT under NISER. In 2008, the Malaysian cabinet decided to spin-off NISER from MIMOS Berhad and, make it a separate entity under the Ministry of Science, Technology & Innovation Malaysia. In the early days, NISER functioned as a technical provider to support the government of Malaysia in the implementation process of the National Cyber Security Policy (NCSP). In 2007, NISER was rebranded and was from then on called CSM. Under CSM there are various sub-divisions for taking care of the cyber environment in Malaysia. One of the sub-divisions of CSM is Outreach and Capacity Building Division. These sub-divisions are responsible for educating and improving awareness of Malaysians on the security aspects of Internet usage through an initiative program known as cybersecurity awareness for everyone (CyberSAFE). The objective of CyberSAFE is to convey the necessary practical knowledge, information and resources on cyber safety in order to enhance the cybersecurity. Thus, training and cybersecurity awareness sessions were conducted for several age groups of kids, youth, parents and organisations (CyberSecurity Malaysia, 2012). Besides the responsibility of educating and improving cybersecurity awareness, CSM also acts as a one stop centre in solving Internet security breakdowns such as spam, cyber harassment and cyberstalk.

2.2.2 Cybersecurity awareness approaches, content coverage and target audience

CSM uses a few approaches in conducting awareness to Malaysian citizens. Among the approaches are having an online portal which includes information and tips on necessary

precautions, advice, videos, games, quizzes and newsletters on cybersecurity. Various approaches are used in order to attract the audience to the importance of the cybersecurity message (refer to Figure 2.3). Apart from online portal, CSM also conducts series of cybersecurity awareness program throughout Malaysia targeting different types of Internet users with the objectives to educate and improve cybersecurity among the Malaysian citizens.

The content of the CyberSAFE program is specifically designed towards meeting different types of Internet users such as kids, youths, parents and organisations (refer to Figure 2.2 and Figure 2.3) . Different approaches are used for each type of user. Specifically, the cyber tips for children include messages on basic security protection such as managing cyber friends and safeguarding personal information. Particularly for youngsters, the cyber tips given to them covers information protection, spyware watch, emails and spams, chat safety, blog safety, cyber bullying, password protection, P2P sharing and downloading, making friends online, cyberstalk, cyber harassment, virus, worms and general safety computing tips. On the other hand, cyber tips for parents are more towards how to observe their children while using the Internet. Meanwhile, for organisations, the tips given are focusing more on business continuity and disaster discovery. In this study, the subject of interest is on youngsters and personal data protection. Based on the cybersecurity awareness message conveyed via the CyberSAFE program, personal data protection is highlighted in almost every cyber tips. Therefore, it is suitable for this study to leverage on the CyberSAFE program in order to perform the assessment on personal data protection among youngsters in Malaysia.

Figure 2.2 : Screen Snapshot of Cyber SAFE Malaysia Official Portal (http://www.cybersafe.my/en/)

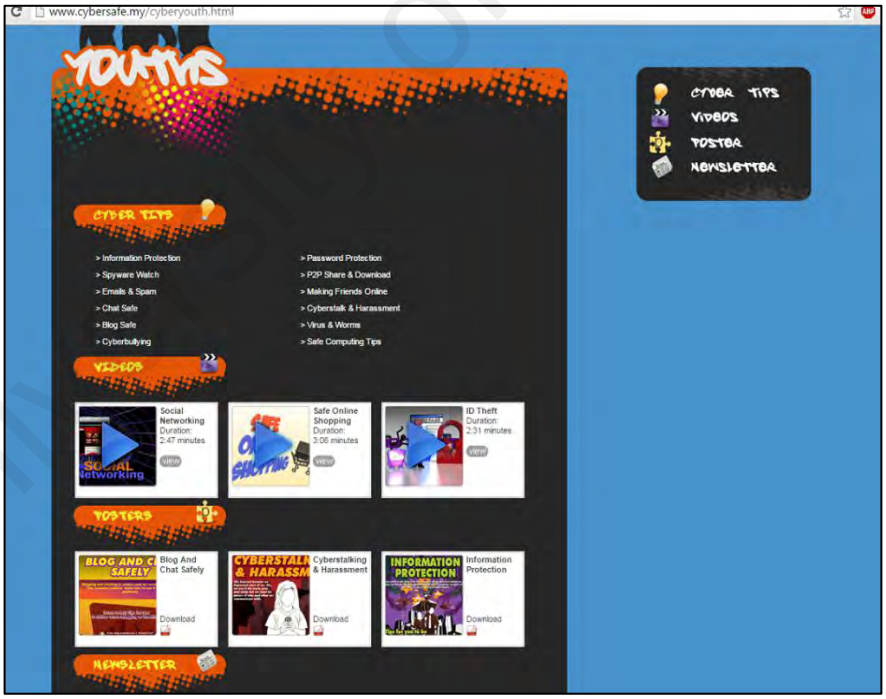

Figure 2.3: Screen Snapshot of Current Delivering Approaches to Youngsters (http://www.cybersafe.my/cyberyouth.html)

2.3 PERSONAL DATA PROTECTION

Personal data defined by the United Kingdon Data Protection Act (1998), refers to living individual information like name, date of birth, address, identification number as well as any expressions of opinions. In Malaysia, personal data protection is defined by the Personal Data Protection Act (2010) as protection towards any information of an individual in commercial transactions which include physical or digital usage of personal data. Personal data is normally captured and recorded for future use and it could also consist of sensitive personal data such as the physical and mental health condition of an individual, political opinion, religious belief, and the commission or alleged commission of any offence. In the digital environment, personal data is widely used and is sometimes available freely without any restrictions (Tene & Polonetsky, 2012). Thus, it is crucial to protect the personal data of individual from being invaded by a third party due to the harmful effects it can cause on individual. In the context of Malaysia, great amounts of personal data are collected from individuals through the physical and digital medium and used for many reasons. In line with sophistication of technology, commercial transactions such as online banking process large amounts of personal data daily. The trend of processing personal data has created concerns regarding how the personal data is being used and any modification or misuse is involved. Thus, the Personal Data Protection Act 2010 was enacted to provide protection against people or groups who processes or authorises the processing of personal data. The provision of law, through the Personal Data Protection Act 2010 in Malaysia, governs Malaysian personal data protection for persons of any age from being victims when they are online (Manap, 2013; Manap, Basir, Hussein, Tehrani, & Rouhani, 2013). The cybersecurity awareness program conducted by CSM also highlights the Personal Data

Protection Act 2010 to inform Malaysian citizens that there is a provision of Personal Data Protection Act which protect their personal data. The following sections discuss several components related to the requirement of personal data protection among youngsters.

2.3.1 Related components involving personal data protection and youngsters

Personal data protection and its relationship with youngsters can be explained by examining three components; i) password management, ii) the usage of social technologies and iii) concerns over privacy. The investigation of personal data protection components is required in order to ensure the correct components being used during the development of proposed conceptual framework.

2.3.1.1 Password management

The responsibility of password management always starts with the process of creating a new password by an Internet user themselves, for new Internet applications. It is somehow considered a simple task to commit to; however, Internet users who are the weakest link in the cyber world often underestimate this simple task (Tam, Glassman, & Vandenwauver, 2010; Bresz, 2004; Leach, 2003). The understanding of creating good and bad passwords is different among people and this has opened possibilities for the password to be discovered by cyber criminals, and consequentially, lead to unauthorised access to individual personal data. Often, the Internet users are advised to change their passwords frequently and the same passwords should not be used for a prolong period of time. However, due to limited cognitive capacity and reasoning ability, Internet users frequently disregard this (Tam et al.,

2010). Apart from that, Internet users also practise sharing password especially among close family members and friends (Meter & Bauman, 2015; Weinstein & Selman, 2014; Kaye, 2011; Singh, Cabraal, Demosthenous, Astbrink, & Furlong, 2007). This practice creates the opportunity for personal data violation. As for youngsters, they lack password management skills. For example, their password is shared among friends without restriction (Rahim, Hamid, Mat Kiah, Shamshirband, & Furnell, 2015; Lenhart et al., 2011). Their focus is only to acquire online connection and disregard the importance of keeping their password to themselves (Vandoninck et al., 2014; Smahel et al., 2012). Another contributing factor which risks their password being exposed is the attitude of youngsters who are always keen and enthusiastic when exploring the Internet. They can unintentionally leave their password revealed to strangers (Correa et al., 2013; Madden et al., 2013; Amanda Lenhart et al., 2010).

2.3.1.2 Social technologies

Social technologies which also referred as Web 2.0 technologies have given tremendous impact to personal data protection (Acquisti, Brandimarte, & Loewenstein, 2015; Spiekermann, Acquisti, Böhme, & Hui, 2015). Through the development of social technologies, the usage of personal data is now varied and the degree of its usage has become extensive. In the example given by Suraya (2013), there is a list of social technologies ranging from blogs, microblogs, wikis, social networking sites, media sharing sites, podcasting and podcasting technologies, social bookmarking sites, really simple syndication (RSS), online games, online discussion forums and instant messaging. Among the most widely used social technologies to youngsters are social networking sites, online

games and instant messaging (Madden et al., 2013; Livingstone et al., 2005). These technologies are the most popular and extensively used by the youngsters. According to Lenhart et al. (2011), while using social technologies, youngsters often left their digital footprint available on the web. The consideration on the effect and impact to their reputation and future life were neglected and jeopardize by this exposure on the Internet. To make matter worse, the impact of social technologies on youngsters is misuse and trust on strangers online which make them expose and being vulnerable to identity theft and cyber harassment (Lucero, Weisz, Smith-Darden, & Lucero, 2014). The main factor contribution to the extensive usage of social technologies is due to the wide use of smartphone devices among youngsters which gives them easy access to the Internet (Lenhart, 2012).

2.3.1.3 Concern over Privacy

Violation of personal data is very much related to violation of individual privacy (Tene & Polonetsky, 2012). The protection over individual privacy is required in order to avoid personal data being used by any third parties either in the physical world or in the digital environment (Odoemelam, 2015; Soffer & Cohen, 2015). Personal data is often kept secret by an individual and only revealed when needed. However, due to youngsters' attitude, their privacy is at risk particularly when they share their personal data among small circle of close friends or even strangers (Shin & Kang, 2016; Gross & Acquisti, 2005). The problem with regard to their willingness to share personal data raises concern on how youngsters perceive their personal data privacy. Youngsters commonly practice exchange of personal data which include birth dates, cell phone numbers, current residential address,

dating preferences, relationship status, their political views and also their hobbies or interests (Lai & Ngerng, 2015; Gross & Acquisti, 2005). This action raised another concern over youngster's privacy as their personal data is freely available over the web. This has indirectly exposed them to vulnerabilities and cyber threats such as identity theft or online paedophilia (Chawki, Darwish, Khan, & Tyagi, 2015; Fire, Goldschmidt, & Elovici, 2014). In addition to this, youngsters are found to be in lack of self-monitoring and not limiting them from exposing too much personal information. Youngsters are also lacking in knowledge on what are the expectation that can result from violation of their privacy (Youn, 2009). In the cybersecurity awareness program by CSM, the message on privacy is always broadcast through sample of cases and youngsters are always reminded that they are protected by a series of laws such as the Communications and Multimedia Act 1998, Computer Crimes Act 1997, Copyright Act (Amendment)1997, Digital Signature Act 1997, Electronic Commerce Act 2006, Electronic Government Activities Act 2007, Payment Systems Act 2003, Personal Data Protection Act 2010, Telemedicine Act 1997, Penal Code (including chapter on terrorism & cyber-terrorism) and Communications and Multimedia Content Code. The purpose of conveying information regarding the laws is to ensure youngsters are aware that their digital activities is monitored, govern by laws and their rights are protected. They also need to be alerted that the Malaysian Government has made this law to ensure harmony digital activities and reduce damages made by cyber criminals.

2.4 SUMMARY OF CURRENT APPROACHES TO ASSESS CYBERSECURITY AWARENESS

This section focuses on discussing the problem statement presented in the previous section 1.2. The discussion was based on previous assessments of cybersecurity awareness

programs by focusing on the previous methodologies used, target audiences and scope of assessment. This section justifies the research gaps found in this study.

2.4.1 Methodology used

The assessment of cybersecurity awareness is not new, as several scholars have already proposed methodologies that are capable of identifying and assessing Internet users' acceptance and understanding levels in relation to security. The identified methodologies are discussed in this section. The main purpose of this section is to identify current methodologies used for assessing users on cybersecurity awareness program and whether any form of program evaluation model has been applied previously.

A literature review was done in cybersecurity awareness assessment method and presented as per matrix analysis (refer to Table 2.1) which encompasses a list of studies on the horizontal lines and identified methodologies on the vertical lines. There are 10 identified distinctive assessment methodologies which are further grouped as quantitative or qualitative methodologies. The value-focused, survey-based and vocabulary test is grouped under quantitative methodologies while observation, interviews, game tools, e-learning, focus groups, document reviews and responses to email are considered qualitative methodologies. The general trends of assessment methods for cybersecurity awareness mainly concern questionnaire-based surveys, which represent quantitative data. Two studies were found to have combinations of both methodologies, including observation, survey, and interviews (Kok et al., 2010; Rezgui & Marks, 2008). The methodology trend encompasses manual assessment, for instance observation, survey and document reviews, and technology-assisted assessment, such as game tools and e-learning. It was also found

that two studies utilised methodologies borrowed from education, namely value-focused and vocabulary tests.

Table 2.1: Matrix Analysis of Assessment Methodologies Identified in Cybersecurity Awareness Program

Methodologies	**Quantitative**			**Qualitative**						
Assessment methods **Authors and Years**	**Value-focused**	**Question-naire based survey**	**Vocabul-ary test**	**Obser va-tion**	**Inter-view**	**Game tool**	**E – Learni-ng**	**Focus group**	**Docume-nt review**	**Response to email**
Kruger and Kearney (2006)	√									
Chen et al. (2006)							√			
Albrechtsen (2007)					√					
Cone, Irvine, Thompson, & Nguyen (2007)						√				
Charoen, Raman, & Olfman (2007)								√		
Drevin, Kruger, & Steyn (2007)	√									
Furnell et al. (2007)		√								
Power (2007)		√								
Rezgui and Marks (2008)		√		√	√				√	
Furnell et al. (2008)					√					
Bulgurcu, Cavusoglu, & Benbasat (2010)		√								
Kritzinger and von Solms, 2010)							√			
Kruger, Drevin, & Steyn (2010)			√							
Talib et al. (2010)		√								
Hagen, Albrechtsen, & Ole Johnsen (2011)							√			
Labuschagne, Burke, Veerasamy, & Eloff (2011)						√				
Furman, Theofanos, Choong, & Stanton (2012)					√					
Rantos et al. (2012)		√								
Slusky and Partow-Navid (2012)										
Caputo, Pfleeger, Freeman, & Johnson (2014)										√
Kim (2014)		√								
Mani, Choo, & Mubarak (2014)		√								
Parsons, Young, Butavicius, McCormac, Pattinson, & Jerram (2015)		√			√					

Through the matrix analysis, cybersecurity awareness assessment basically requires a combination of mixed methodologies, because quantitative methodology has limitation in assessing humans, certain elements require the involvement of qualitative methodologies, such as in assessing human behaviour. The reflection of learning during cybersecurity awareness must be implied to change the Internet user's behaviour. Changes in behaviour require observing human behaviour in reality. Thus, a mix of quantitative and qualitative methodologies is considered effective in designing an approach to assess cybersecurity awareness.

The methodologies applied in the previous studies show a great amount of surveys, which seems to be beneficial in getting immediate responses from users undergoing a cybersecurity awareness program. However, in designing an assessment strategy for evaluating youngsters, it is challenging to obtain valid input. This is because youngsters tend to offer responses that do not fully represent their thoughts due to their limited reasoning and maturity, therefore additional methodologies to extract their feedback is necessary. It would be beneficial to have an assessment strategy that comprises of quantitative and qualitative methodologies to gain feedback. Thus, to ensure that feedback is valid and reliable, the strength of each methodology would complement each other.

This section is supported by Tsohou, Kokolakis, Karyda, & Kiountouzis, (2008), who conducted an analysis on finding assessment approaches to cybersecurity awareness programs, which include several studies identified in the matrix analysis. From their list of reviews, apparently no assessment has ever been conducted using the program evaluation model. The assessment of cybersecurity awareness program is suggested to be clear and

comprehensive by combining multiple perspectives as in program evaluation model to ensure it is effectively investigated and could prevail the actual behaviour among participants (Abawajy, 2014; Crossler et al., 2013). This statement is supported by the latest finding by Donaldson, Siegel, Williams, & Aslam (2015) that also highlighted a systematic framework for assessing cybersecurity awareness program and its compliance requirement. This statement has given added value to our findings on the claim that little attempt been conducted on cybersecurity awareness programs assessment using the program evaluation model. Their study also revealed that the ultimate goal of a cybersecurity awareness program is to change user behaviour and instil a security culture using only a few assessments aimed at enhancing the current cybersecurity awareness module.

2.4.2 Target audiences

The target audience in this section refers to the community targeted in the cybersecurity awareness assessment in previous studies. It is important to know which group of people were targeted in the previous studies, which were left out from the assessment and whether youngsters were part of the target audience. The requirement is to identify youngsters as part of the target audience is due to the fact that this group of people is in a state of potentially exhibiting addictive behaviour towards online technology and Internet applications (Micheli, 2015; Johansson & Götestam, 2004). Youngsters also appear to excessively use the Internet, which leaves them surrounded by Internet vulnerabilities including online fraud and identity theft (Sithira & Nguwi, 2014; Vandoninck et al., 2014). Additional reason for having them as a focal group to be assessed is because in a study by

Boyd (2007), it was found that youngsters are perceived as 'cool' among the school community if they are connected to social media. Thus making youngsters actively seeking ways to get connected and gain many friends via social media. However, in their state of building up a cognitive, social identity and development, they still have lack of security awareness to protect themselves from Internet vulnerabilities (Boyd, 2007; Livingstone et al., 2005).

According to Correa et al. (2013), Youngsters are among the most active Internet users. They are very energetic in exploring Internet resources and engaging in various activities using online media. The consistent finding of high Internet literacy among youngsters as compared to the elderly in studies by Kok et al. (2010) and Livingstone et al. (2005) is another element that justifies the need in focusing toward youngsters in gaining appropriate security awareness. Their enthusiasm in exploring the Internet often exposes them to risks of cyber threats, such as phishing and identity theft (Furnell, 2010). The other reason for conducting assessments among youngsters is the lack of awareness of safety measures, security practices, and reliability of Internet applications used (Furnell, 2010; Livingstone et al., 2005). In addition, youngsters have an attitude that overshares their information on online media, thus encouraging third parties or intruders to stalk or steal personal information.

The literature was analysed using matrix analysis, which consist list of studies on the horizontal line, and vertical lines that categorised the target audience into organisations, home users, college/university students, novice Internet users and social networking users (refer to Table 2.2). From the matrix analysis, it was found that in previous studies; most

targeted unit of analysis were organisations and few studies focused on other categories. It was also found that little studies were done on analysing the target audiences based on age distribution, by differentiating people in terms of their age group.

Table 2.2: Matrix Analysis on Target Audiences Identified in Cybersecurity Awareness Program

Target audiences **Authors and Years**	**Organizations**	**Home users**	**College/ University Students**	**Novice Internet users**	**Social networking users**
Kruger and Kearney (2006)	√				
Chen et al. (2006)	√				
Drevin, Kruger, & Steyn (2007)	√				
Furnell et al. (2007)		√			
Albrechtsen (2007)	√				
Cone, Irvine, Thompson, & Nguyen (2007)	√				
Charoen, Raman, & Olfman (2007)	√				
Power (2007)	√				
Rezgui and Marks (2008)	√				
Furnell et al. (2008)				√	
Bulgurcu, Cavusoglu, & Benbasat (2010)	√				
Kruger, Drevin, & Steyn (2010)			√		
Talib et al. (2010)	√	√			
Kritzinger and von Solms, 2010)		√			
Hagen, Albrechtsen, & Ole Johnsen (2011)	√				
Labuschagne, Burke, Veerasamy, & Eloff (2011)					√
Furman, Theofanos, Choong, & Stanton (2012)				√	
Rantos et al. (2012)	√				
Slusky and Partow-Navid (2012)			√		
Caputo, Pfleeger, Freeman, & Johnson (2014)	√				
Mani, Choo, & Mubarak (2014)	√				
Kim (2014)			√		
Parsons, Young, Butavicius, McCormac, Pattinson, & Jerram (2015)	√				

It appeared that none of the studies reviewed focused on youngsters in their assessment. The justification of assessing youngsters as a separate group was discussed in the earlier part of this section. However, it is an important consideration to realise that if the assessment generally groups youngsters into an identified target audience, the assessment will result in more variations and less uniformity to generalise the feedback to represent youngsters.

Cybersecurity awareness programs require proper segmentation of Internet users, because they differ in the levels of security awareness, acceptance, and amount of help they need (Peltier, 2005). The concept of awareness should be tailored to a specific audience and should not be a "one-size-fits-all" approach (Choo, 2011; May, 2008; Valentine & Labs, 2006).

2.4.3 Scope of assessment

The importance of including the understanding of personal data protection as part of the assessment focus on users is due to the issue of identity theft that affects youngsters owing to characteristics discussed in the previous section. Identity theft is one of the fastest growing crimes in cyberspace (Aimeur & Schonfeld, 2011). It happens due to wide availability of personal information on the web, which attracts third parties to steal and use information for illegal purposes or gain personal benefits (Broadhurst & Chang, 2012; Whitson, 2009; WenJie, Yufei, & Archer, 2006). These fraudulent activities usually occur without the owner's knowledge or consent (Loibl, 2005). According to Newman & Mcnally (2005), the anatomy of identity theft encompasses three major stages: (1)

Acquisition stage - normally performed by phishing through social engineering, spamming, "dumpster diving", and spyware activities; (2) Use stage - this occurs, for example, when the stolen identities are used for instant withdrawal and transfer of money, account login, and credit card swiping; and (3) Discovery stage – this occurs when the users become aware that their identity has been stolen. Hence, innocent Internet users become victims of other users who are trying to gain illegal access (Helbing, 2015; Gupta & Kumaraguru, 2014; Newman, 2006).

Investigations on the increasing identity theft among youngsters reveal that youngsters have lack of understanding and harbour lenient attitude towards personal data protection when using the Internet (Walrave, Vanwesenbeeck, & Heirman, 2015; Furnell et al., 2008; Chen et al., 2006). Avid young Internet users become victims, because they are ill-equipped to address Internet threats (Furnell, 2010). This is corroborated by a clinical report on the impact of social media on children, adolescents and families by O'Keeffe, Clarke-Pearson and Council on Communications and Media (2011). They found that among children and adolescents, they are in risk by having inappropriate habits and behaviour in using technology, oversharing attitude and lack of privacy protection. Another factor that contributes to the risky behaviour that leads to identity theft towards youngsters is their perception. Studies have shown that when youngsters perceive a particular site or element in cyber space as beneficial to them, they have higher tendency to share information without any restriction (Shin & Kang, 2016; Youn, 2009).

To combat identity theft especially among youngsters, their understanding of the importance of personal data protection must be identified. Therefore, any studies on current

cybersecurity awareness assessments must determine whether personal data protection is highlighted as an essential part of the assessment. The matrix analysis (refer to Table 2.3) consists of the same horizontal line showing a list of studies and eight (8) identified scopes of assessment. The identified scopes are security in general, level of security awareness, knowledge, attitude, behaviour, information assurance and reporting. The trend seemed to focus on security in general, apart from the level of security awareness, knowledge and participants' attitude.

The relationship between the issues of identity theft that can easily target youngsters and the trend of cybersecurity awareness assessment, there is an evident gap in the focus directed by previous researchers on incorporating personal data protection as part of their assessment. Therefore, in planning for the actual research, the assessment scope will be focused on assessing the youngsters' understanding of personal data protection. This is foreseen as an important aspect to identify whether current cybersecurity awareness, in delivering the right message of how personal data protection, can be well-received by participants.

Table 2.3: Matrix Analysis on the Scopes of Assessment Identified in Cybersecurity Awareness Program

Scope of assessment Author and Year	Security in general	Level of security awareness	Knowledge	Attitude	Behaviour	Information Assurance	Reporting
Kruger & Kearney (2006)			√	√	√		
Chen et al. (2006)	√						
Albrechtsen (2007)						√	
Cone, Irvine, Thompson, & Nguyen (2007)	√						
Charoen, Raman, & Olfman (2007)		√					√
Drevin, Kruger, & Steyn (2007)		√					
Furnell et al. (2007)	√						
Power (2007)	√	√					
Rezgui & Marks (2008)	√						
Furnell et al. (2008)			√				
Kruger, Drevin, & Steyn (2010)		√					
Talib et al. (2010)	√						
Kritzinger & von Solms, 2010)			√		√		
Bulgurcu, Cavusoglu, & Benbasat (2010)	√						
Hagen, Albrechtsen, & Ole Johnsen (2011)						√	
Labuschagne, Burke, Veerasamy, & Eloff (2011)			√	√			
Furman, Theofanos, Choong, & Stanton (2012)		√		√			
Rantos et al. (2012)	√						
Slusky & Partow-Navid (2012)	√						
Caputo, Pfleeger, Freeman, & Johnson (2014)	√						
Kim (2014)	√						
Mani, Choo, & Mubarak (2014)			√	√	√		
Parsons, Young, Butavicius, McCormac, Pattinson, & Jerram (2015)		√					

Although varying methodologies are used in assessing cybersecurity awareness programs, using multiple methodologies in one study is lacking in term of flexibility. Categorising users when assessing cybersecurity awareness program is deemed essential to ensure the right cybersecurity message is delivered to the right audiences. Thus, in terms of youngsters, analysing them as one unit is considered insufficient. As a scope of assessment, it is aimed to assist in combating identity theft, specifically on youngsters, because they are more exposed to this kind of cyber threat and will experience harmful effects not just to themselves but their families as well. The identified gap can be seen as a missed opportunity that may be useful in planning for an effective way to assess youngsters in terms of their feedback and understanding of personal data protection.

2.5 CHAPTER SUMMARY

This chapter discusses the relevant concepts pertaining to this research. It provides a brief introduction to the trend of Internet usage in Malaysia and youngsters particularly. It also deliberates on the characteristics of youngsters in using the Internet. This chapter also review the cybersecurity awareness program and the current approaches in Malaysia. Next, this chapter also focus on discussing important elements on personal data protection. Among the important components are i) password management, ii) the usage of social technologies and iii) concerns over privacy. In order to justify the use of program evaluation model in this study, the review on the current approaches in assessing cybersecurity awareness program is also presented. The approaches mainly concern on the previous methodology used, target audiences and scope of assessment.

The following chapter highlights the theoretical background of the research. The theoretical options available are presented and discussed for nominating an appropriate program evaluation model. The chapter is concluded with a proposed conceptual framework.

CHAPTER 3

THEORETICAL FOUNDATION AND PROPOSED CONCEPTUAL FRAMEWORK

3.1 INTRODUCTION

This chapter discusses the research's underlying theories and begins by covering the theories used in Information Systems (IS) assessment research. Next the discussion on the theories used to guide this research is explained thoroughly. Attention, Relevance, Confidence and Satisfaction Model of Motivational Design (ARCS), Situated Learning Theory (SLT) and Theory of Reasoned Action (TRA) were selected as the central theoretical lens because it provides the necessary prescription to nominate construct on assessment criteria's which further used in selecting appropriate program evaluation model which guided this study. The combination of theories required in assessing cybersecurity awareness program among youngsters in order to identify a comprehensive assessment criteria's. This chapter also discusses the process of selecting suitable program evaluation technique based on the identified construct or assessment criteria's. Lastly, by integrating various insights from the selected theories, mapped with appropriate program evaluation model and components of personal data protection, a conceptual framework is presented. The proposed model is used to facilitate, plan, and design the overall research.

3.2 THE IMPORTANCE OF THEORY

Theory is an important element in research because it is a systematic view of phenomena to answer and explain research questions (Creswell, 2009). According to Gregor (2006), the classification of theory are as the following.

Analysis and description: The use of theory to describe and observe a phenomena, its relationship between constructs and making generalisations.

Explanation: The use of theory upon phenomena of interest by making a query on why, when, how things happen and its causalities.

Prediction: The use of theory to forecast future consequences based on certain conditions and it will be represented in a probabilistic manner.

Prescription: The use of theory to provide explanation upon a technique or structural that is being used to construct a certain studied artefact.

Specifically, the role of theories in this research is used as prescription. The prescription in this study context is referring to the use of theories in the identification process of assessment criteria's. The assessments criteria's found in the theories were used to select the appropriate program evaluation model which then will be used as constructs for an assessment of cybersecurity awareness program among youngsters. This research does not aim to analyse, describe, explain or predict the assessment of cybersecurity awareness program. However, the results from using theories as prescription for cybersecurity awareness assessment might be useful in offering some useful recommendations such as the enhancement module on personal data protection among youngsters and framework for

future assessment. In the following sub-sections, the theories adopted in assessment of IS and specific theories selected for this research are discussed.

3.2.1 Theories in assessment of Information Systems (IS) Research

As this research is focusing on assessment, theories pertaining to the assessment of Information Systems should be reviewed to determine the research investigation. Studies that focused on individual assessment of IS were largely drawn from the Technology Acceptance Model (TAM), the Unified Theory of Acceptance and Use of Technology (UTAUT), Information Processing Theory and IS Success Model. The following theories were reviewed accordingly and its summary is presented as per Table 3.1 below.

Table 3.1: Theories used in Assessment of Information System

Theory	Description	Construct or variable	Assessment level	Authors
Technology Acceptance Model (TAM)	Perceived usefulness and perceived ease of use determine an individual's intention to use a system.	Perceived usefulness, perceived ease of use and behavioural intention to use.	Individual	(Davis, & Venkatesh, 1996; Davis, Bagozzi, & Warshaw, 1989)
Unified Theory of Acceptance and Use of Technology (UTAUT)	Explain user intentions to use an IS and subsequent usage behaviour.	Performance expectancy, effort expectancy, social influence, facilitating conditions, gender, age, experience, voluntariness of use, behavioural intention and use behaviour.	Individual/ Organizations	(Venkatesh, Morris, Davis, & Davis, 2003)
Information Processing Theory	Focusing on mental development and maturity	Sensory input, Short term memory and long term memory.	Individual	(McClelland, Rumelhart, 1987; Miller, 1956)
IS Success Model	Understanding of success in IS usage	System quality, information quality, user, user satisfaction, individual impact, organisational impact.	Individual/ Organizations	(DeLone, & McLean, 1992)

Examples of theories constructs or variables suggested in IS theories are shown in table 3.1 which include the assessment of individual technology usage and mental development. However the focus of the theories' application in empirical research is meant to be comprehensive and not limited to technology usage only. In addition, most of the theories cited above are positivist-oriented which are suited for a quantitative research approach. Hence, while these theories are relevant as prescription to nominate assessment criteria's for an assessment of cybersecurity awareness program, this research in nature is using mixed method strategy (a further discussion of this is covered in Chapter 4). Thus the suitability of these theories is limited to be considered for a mixed method research. Moreover, as indicated in Chapter 1, the aim of this research is to explore a number of questions, including the identification of assessment criteria's (the "what" question), the employment of proposed framework and its verification (the "how" questions).

Besides, a huge limitation among these theories is the focus on behaviour in which as assessment of program shall not limited to only behaviour but rather to include learning and reaction of individual as well. Therefore, it was decided that combining several theoretical insights is more beneficial in using theory as prescription in this research. In particular, the research employs the ARCS, SLT and TRA. Another reasons for combining ARCS, SLT and TRA is due to the nature of the research which require (a) comprehensive and multiple perspective assessment criteria's (b) the coverage of assessment which include behaviour as well as learning and reaction perspective.

3.3 ARCS MODEL OF MOTIVATIONAL DESIGN THEORY

ARCS Model was initiated by John Keller in 1987. This model is originally based on Tolmah's and Levis's Expectancy Value Theory. The purpose of this theory is to understand major influence in learning motivation. It consist of four human motivation factors which are Attention (A), Relevance (R), Confidence (C) and Satisfaction (S). ARCS are represented in the form of intersection between A, R, C, S and learning motivation in the middle as per Figure 3.1. All these elements are interrelated and have equal weight. The establishment of all components needed to ensure learner is motivated to learn. Attention is referring to sustain learner interest to participate in learning. Thus Keller also suggested in order sustaining the learner interest, the component of perceptual arousal such as using surprise, inquiry arousal (problem to solve and variability) and variety of teaching method.

The next component is relevance which require learner to find the learning has motives and accordance to their interest. In order to achieve relevance in learning process, learner should be clear with goal orientation (how knowledge help them) motive matching (learner) choice and preferences), familiarity (related to learner experience). The next component in ARCS is confidence which refers to the development of positive expectation in achieving success. The component under confidence constitutes performance requirement, success opportunity and personal control. The next component is satisfaction which refers to reinforcement and reward to learn. It can be in the form of intrinsic reinforcement (enjoyment), extrinsic reward (real reward) and equality (equal success factor).

Since 1987, the application of Keller ARCS has been widely accepted and applied to various field such as clinical and education. The purpose of applying ARCS previously is

mainly focusing to obtain learner feedback. In recent years, ARCS is still applicable in which it has been used to access motivational factors in playing online games (De Troyer, Van Broeckhoven, & Vlieghe, 2017; Osma Ruiz, Saenz Lechón, Gutiérrez Arriola, Argüelles Álvarez, Fraile Muñoz, & Marcano Ganzo, 2015). In particular, the application of ARCS among youngsters involved in examining learning style in education (Rani, & Shukla, 2012)

The review made for ARCS in literature shows that it fits the requirement of having learner feedback and it's applicable to be applied among youngsters. The component of ARCS is chosen as the first four assessment criteria's which further used to select appropriate program evaluation model in this study. The components again are attention, relevance, confidence and satisfaction.

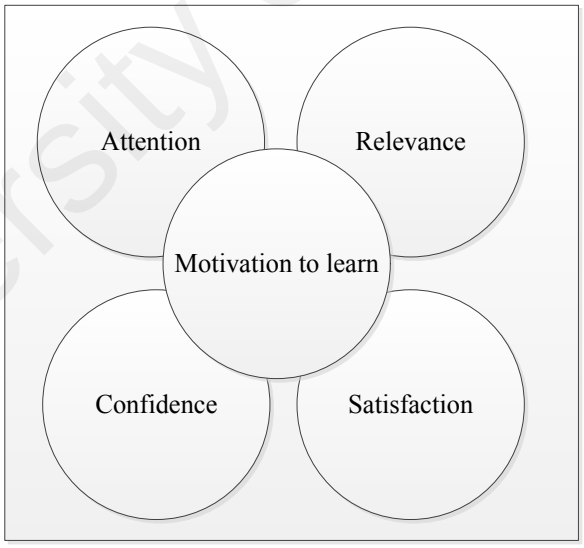

Figure 3.1: ARCS Model (John Keller, 1987)

3.4 SITUATED LEARNING THEORY

SLT was developed by Jean lave in 1988, this theory posits that learning will take place unintentionally and situated with embedded authentic activity, context and culture. Lave also acknowledge SLT as "legitimate peripheral participation" which refers to knowledge that can be gained through authentic context or setting. SLT is represented in the form of diagram in which activity, context and culture are used to explain how multiple process of learning take place. The illustration of SLT is depicted in Figure 3.2. The application of SLT for this study is due to the scope of the assessment that includes learning perspective.

The used of SLT has been widely accepted in evaluating learning capacity on individuals which also justified the use of theory within the context of this empirical research. Particularly on youngsters, the SLT has been used in school assessment as in the study by Korthagen (2010). Therefore, the component in SLT is added into the list of assessment criteria's that will be used to select the suitable program evaluation technique for this study.

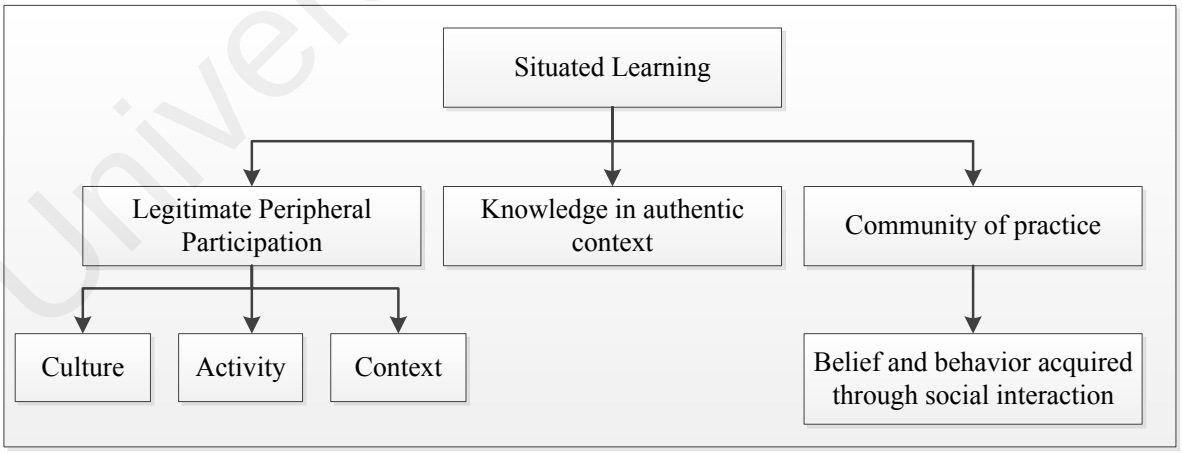

Figure 3.2: SLT (Jean Lave, 1988)

3.5 THEORY OF REASONED ACTION

The final theory in selecting suitable program evaluation technique in this study is TRA. TRA is among the classic model of persuasion which developed by Martin Fischbein and Icek Ajzen in 1967. It was originated from the theory of attitude. This theory explains the relationship between attitude and behaviour which constitute human actions. TRA basically is composed of four components that explain behaviour prediction of an individual as depicted in Figure 3.3. The first two components is attitude towards act or behaviour and subjective norm. These two components established the behavioural intention of an individual which further led to actual behaviour. For example, attitude of an individual often lead to a certain behaviour but it is subjected to relevant norms or strength of belief which provide suggesting alternative that could influence the actual attitude of an individual.

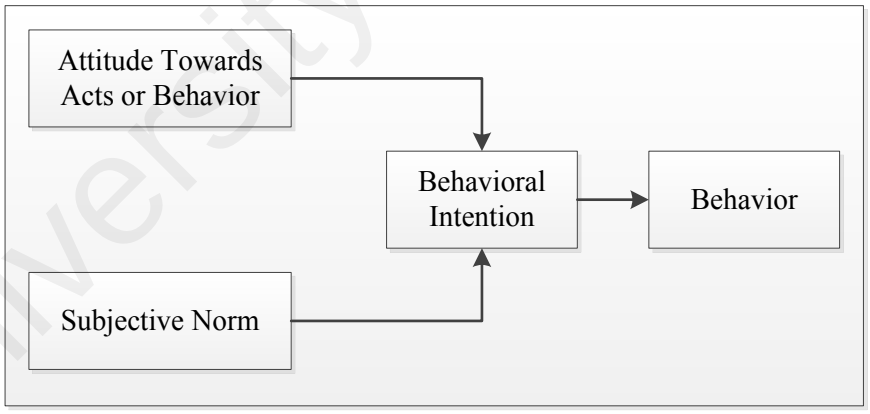

Figure 3.3: TRA (Martin Fischbein and Icek Ajzen, 1967)

The used of TRA has been widely accepted since its first introduction until present day. It is also a foundation for the well-known Theory of Planned Behaviour (TPB) which was

also proposed by Icek Ajzen later in 1985. The four component of TRA is used is selecting the suitable program evaluation model.

Based on the review made to the relevant theory in this study, there are lists of assessment criteria's that provide foundation in selecting the program evaluation model. The summary of theory and identified assessment criteria is presented in Table. 3.2. In the next section, the discussion on program evaluation technique and its models is discussed accordingly.

Table 3.2: List of Identified Assessment Criteria's

Relevant theories	Assessment criteria's
ARCS Model of Motivational Design Theory	Motivational: attention, relevance, confidence and satisfaction
Situated Learning Theory	Learning: context, activity and culture
Theory of Reason Action	Behaviour: attitude towards act, subjective norm and behaviour intention

3.6 PROGRAM EVALUATION TECHNIQUE

This section provides a brief introduction on program evaluation technique together with its benefit, rationale and limitation. Program evaluation was defined by Scriven (1967) as "a methodology used to determine the worth, value and merit of an object which referred to a program, theoretical project or entire entity that qualified to undergo evaluation or assessment" (p. 39-83). Program evaluation involves systematic investigation and dynamic procedures in conducting the evaluation for the purpose of judgment, decision making,

improvement, and program upgrading (Rossi et al., 2004; Royse et al., 2001; Yarbrough et al., 2011). A program evaluation technique is useful for evaluating a program that has the involvement of user (Royse et al., 2001). The basic idea of using this technique is to determine whether a program is able to achieve its objective, its effectiveness, and whether the inputs obtain can be used for future enhancements.

As one of the applied research techniques, the early days of the program evaluation technique was used in assessing the involvement of education and public health (Fitzpatrick, Sanders, & Worthen, 2004; Rossi et al., 2004). Presently, the usage of program evaluation has grown and many fields have benefited from this technique as it can be systematically used for seeking facts based on a conducted program (Royse & Thyer, Padgett, 2015; Mertens, & Wilson, 2012). The continuous development of the program evaluation technique has transformed it to a systematic and extensive approach that can be used in various fields, including science and technology. As a trans disciplinary technique, program evaluation has positive effects on other fields, such as Information Technology (IT), management, human resources, public administration, clinical psychology, and health (Louw, 2012; Madaus, Scriven, & Stufflebeam, 2012). This technique normally consists of different phases of data gathering, data analysis, and evidence interpretation regardless of the methodology used. The interpretation phases provide inputs for the program modules improvements and policies. The continuation or suspension of a program can also be determined in this phase. Furthermore, this technique can be used as a planning tool to identify the elements that should be included, the manner of activities that should be

delivered, and the expected changes required (Newcomer, Hatry, & Wholey, 2015; Mertens, 2014; Louw, 2012).

Educational program evaluation started with a linear causal model of evaluation techniques, including the causal relationship between program elements and desired outcomes (Frye & Hemmer, 2012; Stufflebeam, & Shinkfield, 2007). A linear model involves a basic cause and effect model to explain the relationship between the program being studied and its effect. However, this technique has transformed into a dynamic technique, thus leading to the specialisation of the evaluation process in accordance with the corresponding field to cope with human reasoning complexity and recent technology requirements. This transformation has resulted in a new paradigm of evaluation techniques by integrating Program Theory, Theory-driven evaluation approach, and Social Science Theory to form new evaluation models and approaches (Royse & Thyer, Padgett, 2015; Frye & Hemmer, 2012; Mertens, & Wilson, 2012).

According to Fitzpatrick, Sanders, & Worthen (2012), Rogers, Petrosino, Huebner, & Hacsi. (2000), Program Theory refers to a model that helps to visualise the inputs and expected outputs of a program. Program theory is also referred to as the logic model (Donaldson, 2012; Yampolskaya, Nesman, Hernandez, & Koch, 2004; Cooksy, Gill, & Kelly, 2001). Program theory supports the evaluation components, and this type of evaluation model is called the theory-driven evaluation approach. The integration in this approach dynamically derives the formative and summative information from the object

being evaluated (Mertens, & Wilson, 2012). Articles on program evaluation techniques are reviewed and presented in Table 3.3 below.

Table 3.3 : The Usage of Program Evaluation Technique

Author	Field	Research method	Purpose
Butler et al. (2014)	Health	Mixed	To promote transparency
Beirness and Beasley (2014)	Traffic injury	Quantitative	To find comprehensive findings
Brown, Dunn, & Budney (2014)	Child and adolescent abuse	Quantitative	To revealed the level of knowledge
Robbins, Pfeiffer, Wesolek, & Lo (2014)	Health	Mixed	To find comprehensive findings
Yeh et al. (2014)	Computer methods and program	Quantitative	To evaluate an online system
Akhurst and Lawson (2013)	Health (therapy and rehabilitation	Qualitative	To identify a relationship between the parameters defined and desired action for improvement.
Cass et al. (2013)	Public health	Mixed	To measure intervention and efficiency of management
Farmer and Reupert (2013)	Health	Mixed	To increase the confidence level of the individual.
Johnson, Hall, Greene, & Ahn (2013)	Program evaluation	Qualitative	To predict social world that is not fixed and stable
Pogrund, Darst, & Boland (2013)	Education (visually impaired)	Mixed	To capture the experience and opinion of each respondent for making future enhancement to the program.
Reynolds and Sutherland (2013)	Health	Qualitative	To aid decision making process
DiVall et al. (2012)	Education (pharmaceutical)	Mixed	To identify the required improvement.
Banjok, Puddester, MacDonals, Archibald, & Kuhl (2012)	Nursing	Mixed	To evaluate a team
Keay et al. (2012)	Public health	Mixed	To avoid bias and underreporting of the situation.
Higgins et al. (2012)	Nursing	Mixed	To find factors for improvement
Clement and Bigby (2011)	Sociology	Qualitative	To assess the program implementation and its outcomes
Galliers and Huang (2011)	Information system	Qualitative	To determine commonality between two entities.
Ho et al. (2011)	Health (mental)	Qualitative	To identify the required improvement.
A'Campo, Spliethoff-Kamminga, Macht, The Edupark Consortium, & Roos (2010)	Medical	Quantitative	To evaluate the feasibility and adaptability of a program.
Ilesanmi (2010)	Architecture	Quantitative	To enhance skills and minimize dissatisfaction as much as possible.
Laven, Ventriss, Manning, & Mitchell (2010)	Environmental management	Qualitative	To guide for detail enquiry
Nabukenya, Van Bommel, Proper, & De Vreede, (2009)	Business and organization	Qualitative	To assess large scope of scenario

Based on the reviews, the adoption of program evaluation involves multidisciplinary fields thus explaining its flexibility to be adopted as the assessment technique in this study. From the perspective of research method, program evaluation could be used either by quantitative or qualitative methods. This gives flexibility for researchers to choose appropriate methods as a way to gain real facts based from the program being studied. In terms of its purpose, the reason underlying the adoption of the program evaluation technique varies but the ultimate aim is to assess and determine outcomes based on the program being studied. To complete a discussion on program evaluation, the following sections present the benefit, rationale and limitation of using program evaluation technique in previous study.

3.6.1 Benefit of program evaluation

Based on the reviewed studies in previous section, information on program evaluation is further explored in terms of its benefits. In order to better understand the benefits, it has been divided into 7 categories which are discussed one by one. Particularly, the category of benefits are categorised as (i) evaluation of program effectiveness, (ii) evaluation of satisfaction, (iii) determining the depth of information, (iv) per individual evaluation, (v) understanding the relationship of program components, (vii) evaluation of intervention study, (ix) measure confidence, knowledge and attitude. The category is referring to topics of interest that were derived on the basis of similarities found from benefits of the previous program evaluation study.

3.6.1.1 Evaluation of program effectiveness

In the studies by A'Campo et al. (2010), Cass et al. (2013), Clement & Bigby (2011), Higgins et al. (2012), Ho et al. (2011), Keay et al., 2012; Laven et al., 2010; Pogrund et al., 2013; Reynolds & Sutherland, 2013), it was shown that the main purpose of adopting the program evaluation method was to determine the outcome and effect of the program on the audience. The selection of the program evaluation technique includes a systematic method of conducting the evaluation. The systematic method contains elements of evaluation that can assist the researcher in analysing elements independently. Different elements being assessed could assist in explaining programs which might be seem effective as a whole, but to a certain degree the elements might be scoreless which require attention. Therefore, an evaluation procedure that is based on the elements can be used to determine the parts that require improvement.

3.6.1.2 Evaluation of satisfaction

The next focus is on the category of evaluation of satisfaction Pogrund et al., (2013) and Ilesanmi (2010). Individual satisfaction is subjective, even though the same program content was used. Thus, by having a program evaluation technique, the satisfaction level of individual can be further analysed to determine the level of acceptance and understanding the program content.

3.6.1.3 Determining depth of information

The category of determining the depth of information can be found in studies by Beirness & Beasley (2014), DiVall et al. (2012), Galliers & Huang (2011) and Pogrund et al. (2013). This benefit is perceived as an advantage provided by the program evaluation technique due to the generalise information it provided.

3.6.1.4 Per individual evaluation

The category of per individual evaluation can be found in a study by Pogrund et al. (2013). From the researcher's perspective, the use of the program evaluation technique in determining individual comment will provide specific information on individual feedback. Although individual evaluation may only be useful if the sample size is small, it can be used to derive a concrete report of assessment.

3.6.1.5 Understanding the relationship of program components

The subsequent discussion is focused on the category of understanding the relationship of program components. This theme can be found in studies by Akhurst & Lawson (2013), Beirness & Beasley (2014), Brown et al. (2014) Butler et al. (2014), Nabukenya et al. (2009) and Reynolds & Sutherland (2013). The program evaluation technique is also beneficial in determining the relationships between the program components, for instance, the relationship of program input and output, which could lead to better prediction of

program effectiveness. The understanding of program components by program evaluation can also justify whether the program is efficient or not. Given that program evaluation composed of systematic methods of conducting evaluation, sample size is not an issue because researchers can use the existing evaluation model and complement and adjusting it to the sample number. When the sample size is large, researchers can plan accordingly prior to the start of the evaluation until the results are achieved.

3.6.1.6 Evaluation of intervention study

Category of evaluation in the intervention study can be found in Keay et al. (2012), Robbins et al. (2014) and Yeh et al. (2014). In developing an assessment strategy for a program, the attempt is to generate a new concept of improvement to the current practices on how the program is conducted. To adopt a program evaluation technique, measurement of the improvement can be revealed. Program evaluation is capable of revealing variations and determining whether a particular new concept or improvement can result in a positive or negative way, which could help the researcher in deciding whether the existing program should be modified or not. From the participant's perspective, the result from the evaluation can help in constructing program content that is more suitable to their needs.

3.6.1.7 Measure the confidence, knowledge and attitude

In addition to the aforementioned category, program evaluation can be beneficial in terms of the following: increasing the confidence level, knowledge and attitude.

3.6.2 Rationale of program evaluation

The same studies (refer to table 3.3) are used to identify rationales of using the program evaluation technique. For better understanding, the identified rationales were further categorised into the following groups: (i) program improvement, (ii) planning tools and (iii) systematic collection.

3.6.2.1 Program improvement

Program improvement is the main reason of using the program evaluation technique by looking into the following reasons; evaluating individual opinion, improvement of service and outcome, improvement of knowledge and skills, program outcomes, efficiency of resource management, policy and decision making, prediction and planning, and better services (Brown et al., 2014; Butler et al., 2014; Akhurst & Lawson, 2013; Cass et al., 2013; Farmer & Reupert, 2013; Reynolds & Sutherland, 2013; Banjok et al., 2012; Higgins et al., 2012; Clement & Bigby, 2011; Laven et al., 2010; Nabukenya et al., 2009). By using the program evaluation technique, the result of the logical relationship of the program input and output is targeted into positive outcome. However, any loopholes identified along the evaluation procedure can assist in proposing a better program that can result in a positive outcome of the program and assist any decision making process.

3.6.2.2 Planning tools

Planning tools is referring to the usage of program evaluation technique in the future planning of a program, tools for evaluating variation, and tools for identifying factors (Robbins et al., 2014; Yeh et al., 2014; Ho et al., 2011; Ilesanmi, 2010). The assessment of the program requires a planning tool to ensure the reliability of all the steps taken and the quality of the evaluation results. Thus, the program evaluation technique can be considered as a good platform of planning tools to assist researchers in making preparations. Furthermore, the program evaluation technique can help to determine in advance regarding the input and context of the program conducted. Variations from the previous method of conducting the program are essential inputs to plan for a better program arrangement inclusive of the program content and flow. Planning tools, in the sense of identifying factors that can affect programs, can also result in a positive value to the use of the program evaluation technique. It can be in terms of tools that can result in the effective development of program assessment.

3.6.2.3 Systematic Collection

Systematic collection encompasses continuation of evaluation, unity of data for concrete evaluation results, minimisation of bias in evaluation results, and addressing the evaluation message in a systematic manner (Beirness & Beasley, 2014; Johnson et al., 2013; DiVall et al., 2012; Keay et al., 2012; A'Campo et al., 2010). The program evaluation technique has models that can be adopted by the researcher in evaluating a program. Therefore, the

specific steps and procedures are already constructed. The researcher may select the suitable models and adjust the models accordingly to meet the nature of the program. The selection of a program evaluation model is useful in the continuation of evaluation because an evaluation should be conducted in a consistent manner and should not be a one-off practice. The use of program evaluation technique can also ensure the unity of the data collected and analysed in a systematic manner, thus resulting in concrete and minimized biasness in the evaluation result.

3.6.3 Limitation of program evaluation

Further investigation is made towards examining the limitation of program evaluation based on the same studies and reveals the following categories of limitations; (i) program evaluation models used, (ii) uniformity of input, (iii) unmatched program evaluation technique, (iv) evaluation period, (v) sample size issue, (vi) input that reflects the generalisation, (vii) nonparticipation, (viii) selection of evaluation method, (ix) methods of presenting the evaluation results, (x) agreement of stakeholders and (xi) segregation of evaluation components.

3.6.3.1 No standard program evaluation model used

The first limitation is that no standard program evaluation model is used (Beirness & Beasley, 2014; Brown et al., 2014; Pogrund et al., 2013; DiVall et al., 2012; Galliers & Huang, 2011). Some studies were evaluated without adopting a proper technique on

program evaluation. Such studies normally defined their own evaluation design and evaluation instrument.

3.6.3.2 Program evaluation results

The focus now is on the limitations of the program evaluation results. These limitations include uniformity of input: the input shall reflect the generalisation, methods of presenting the evaluation results, and agreement of various stakeholders. These limitations can be found in studies by A'Campo et al. (2010), Akhurst & Lawson (2013), Butler et al. (2014), Ilesanmi (2010) and Reynolds & Sutherland (2013). The quality of the program evaluation results can be evaluated on the basis of the quality of the input gathered during the evaluation process. Therefore, the selected components to be evaluated should be precisely defined to ensure the uniformity of input. An input of program evaluation must not be subjected to any boundaries because it must have the capability to be generalised in understanding the larger concept of other program evaluation techniques. In the limitations of presenting the evaluation results and agreement of various stakeholders, the researcher should first identify the requirement and interest of each stakeholder. Thereafter, the researcher can present the evaluation results correctly to the stakeholder.

3.6.3.3 Other limitations

Other limitations were grouped and discussed together under the limitation of the program evaluation context. These limitations include selection of the evaluation method, unmatched program evaluation technique, evaluation period, sample size issue,

nonparticipation, and segregation of evaluation components (Robbins et al., 2014; Yeh et al., 2014; Cass et al., 2013; Farmer & Reupert, 2013; Higgins et al., 2012; Keay et al., 2012; Ho et al., 2011; Laven et al., 2010; Nabukenya et al., 2009). The limitation of the program evaluation context often results in failure in designing and constructing the program evaluation procedures. Every angle of the program evaluation, for example, model selection, timeline, sampling, participation, and component evaluation, should be planned. If necessary, an initial study prior to the actual program evaluation is required. The context of the program evaluation will determine the quality of the evaluation results and any further analysis of the evaluation results. Therefore, the researcher should consider incorporating the required angle precisely prior to the program assessment.

The review on benefits, rationales and limitations are aimed at providing an overview of knowledge and facts of the program evaluation concept and expectations in terms of its best practices. Program evaluation is not merely an exercise that comes at the end of any program, but it is a powerful tool for formal assessment, decision making, and providing the direction of improvement in different aspects of program. Throughout the search process, it was determined that program evaluation has been extensively used in the field of health and education but less consideration in the IT field. Thus, this study attempts to expand the use of program evaluation technique in the IT field by performing an assessment of cyber security awareness programs among youngsters with the application of this technique. A few points should be taken into consideration; selection of evaluation models shall meet the objective of the assessment. This is because the entire assessment is derived based on the selected evaluation model, starting from understanding the component

of assessment, drafting the instrument, sampling procedures, interventions (if any), data analysis and also final findings. Furthermore, the selected evaluation model could also assist in providing quality assessment and suggestion for improvements of the structure and module of cybersecurity awareness programs.

The rationale of conducting program evaluation can differ from one organisation to another. The rationale of using program evaluation is based upon respective stakeholder's opinion and the potential benefits of the evaluation results. For the assessment of the cybersecurity awareness program, the rationale of having a program evaluation technique is to provide improvement to the current state of the cybersecurity awareness program. The improvement is mainly referring to improve the behaviour, knowledge, skills and outcome. Therefore, in the context of cybersecurity awareness program assessment, the drivers of improvement shall be set to improve the state of user knowledge on personal data protection.

Program evaluation has significant benefits and the compatibility of its application in different field is proven. During the assessment of the cybersecurity awareness program, program evaluation can be used to obtain in-depth information on the program, which would later help in the generalisation of information. Furthermore, program evaluation indirectly helps respondents to increase their knowledge by discovering and obtaining new information during the assessment. As a planning tool, program evaluation can assist in formulating strategies in assessing the cybersecurity awareness program and in identifying the purpose and component that require evaluation. Although program evaluation is able to

cater to different requirements in different fields, it needs a proper evaluation design that is applicable in a particular field. Thus, by having the discussion as stated above, the development of the assessment strategy for the cybersecurity awareness program should consider selection of appropriate program evaluation model that meets the requirement to gain feedback from youngsters on the understanding of the cybersecurity awareness program. This is to ensure that information on personal data protection will be delivered.

3.7 PROGRAM EVALUATION MODELS

This section discusses program evaluation models in terms of its name, which developed the application of the components of assessment, aims or objectives as well as the program assessment suitability. According to Mertens, & Wilson (2012), program evaluation models were derived from a combination of Program Theory, Social Science Theory and Evaluation Theory. Program theory was originally developed based on the logical assumption or logic model which could be represented in the form of a diagram by stating the connection between program input and its desired output (Mertens & Wilson, 2012) as depicted in Figure 3.4.

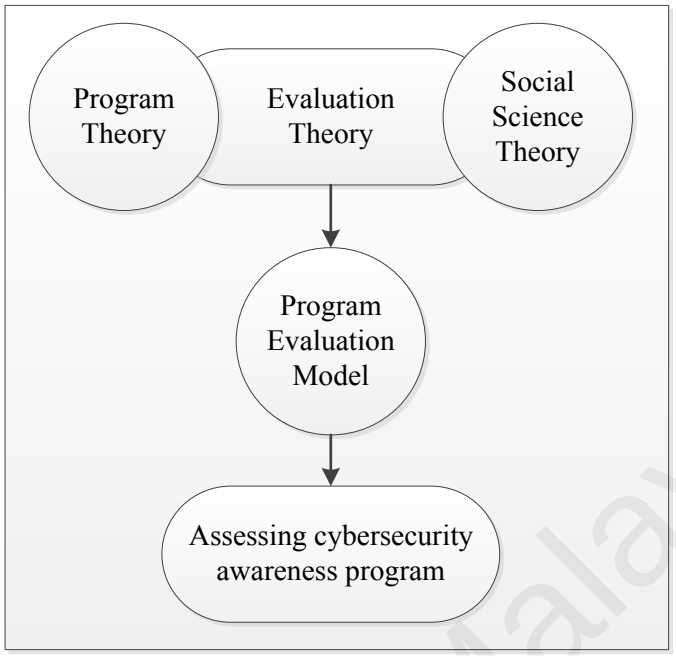

Figure 3.4: Overview of underlying theories of program evaluation models and its relationship to the current research

It provided the basis for constructing the assessment design, selection of questions as well as explaining the assessment results (Rossi et al., 2004). Based on Figure 3.4, program evaluation models derived from Program theory that complements the Social Science Theory by bringing the focus of assessment to the specific needs of stakeholders such as in human development, learning, motivation, literacy development, changing behaviour and other social aspects (Mertens & Wilson, 2012). Meanwhile, the Evaluation Theory refers to the use of value questions in determining the worth of a program (Shadish, 1998). Evaluation theory has several components that require an evaluator to comply and follow the steps prior to calling it as a good evaluation theory. According to Scriven (1967), there were nine elements in forming a good evaluation theory. Firstly, the assessment shall be undertaken in a systematic way. Secondly, the evaluation conclusion that has been done

based on a different design shall be presented in the form of ranking, grading or scoring. Thirdly, the recommendation or justification shall consider other elements such as organisational structure and not be restricted to the evaluation data only. Fourthly, Scriven stressed upon the evaluative investigation. Fifth, evaluation is a trans disciplinary tool that can serve different educational fields. Sixth, the term of evaluation can serve different fields which include program evaluation, performance evaluation and technology assessment. Seventh, every evaluator must independently have their own theories and methods of doing evaluation. Eighth, evaluators can come from many disciplines and lastly Scriven also stressed that evaluation skills shall be applied in many activities such as planning, goal-clarifying and trouble-shooting. In addition to the Scriven components of evaluation, Shadish, Cook & Leviton (1991) proposed a component of good evaluation practices as follows; "knowledge, usefulness of knowledge, valuing, practice and social programming". As opposed to Stufflebeam and Shinkfield (2007), the evaluation theory shall be composed of "overall coherence, core concepts, tested hypotheses on how procedures produce desired outcomes, workable procedures, ethical requirements and general framework for guiding program evaluation practice and conducting research on program evaluation" (pp. 63-64). From the Evaluation Theory, there are several program evaluation models and each of it's differs in term of assessment components, aims and suitability of program. Thus, in this study, one of the program evaluation model is nominated to be use in proposing a conceptual framework. The criteria for selecting program evaluation model in this study must be based on the assessment criteria's identified earlier. The evaluation models that are derived from the above mentioned theories are presented as per Table 3.4.

Table 3.4: Various Program Evaluation and Models

Model	Developer	Components	Aims/Objective	Suitability of program
Kirkpatrick's Four Learning Evaluation Model	Kirkpatrick, (1975)	Reaction, Learning, Behavior and Results	Provide logical, practical and useful methodologies for capturing user perceptions and reactions	Training
Theory-Based Evaluation	Chen & Rossi (1980)	Assumptions of elements for successful program	Combine of the social science theories and stakeholder theories in identifying elements that required for the program to be success	Any program
Experimental & Quasi-Experimental Design	Not available	Understanding the construct between independent and dependent variable.	Comparison between intervention and non-intervention groups.	Any program
Discrepancy Evaluation Model	Provus (1971)	Program Design, Program Operation, Process, Program Interim Product and Program Terminal Products and Program Cost	Examination of program across its developmental stages. The measurement will be based on standards and objectives.	Training
Transaction Model	Stake (1977)	Activity among evaluators and participants	Evaluation process will be combines with monitoring session. Regular feedback sessions are required.	Project activities
Goal-Free Evaluation Model	Scriven (1991)	Methodological studies and process	No objective to avoid biasness. The conclusion will be drawn based on the observation.	Any program
Systematic Evaluation	Rossi and Freeman, (1993)	Is the program reaching the target population? Is it effective? How much does it cost? Is it cost effective?	Focus on analyzing a program to ensure its effectiveness.	Training that require cost
Responsive Evaluation	Stake (1991)	Preliminary report that based on Observation, Time & Place	The evaluation is done based on the stakeholder feedback. The evaluator will be responsive to the stakeholder request and interest.	Promotion

Table 3.4 continued: Various Program Evaluation Techniques and Models

Model	Developer	Components	Aims/Objective	Suitability of program
Connoisseurship Evaluation	Eisner (1979)	"Phenomenological philosophical stance"	The evaluation is conducting via writing upon critics to the studied phenomenology.	Document Evaluation
Quasi-Legal Approach	Not available	Witness called to tender and testify evidence.	For inquiry manner. Not suitable for evaluating training and developmental activities.	Court
Art Criticism Model	Eisner (1997)	Evaluator judgments	For critical reflection and/or improved standard.	Pre-program
Adversary Model	Not Available	Individual evidence	Decision will be based on the judged evidence.	Program
CIPP Model	Stufflebeam (1985)	Context Input Process Product	Based on the concept "Evaluation is to improve not to prove".	Program
Cervero's Continuing Education Evaluation	Cervero, 1998	Program design and implementation, Learner participation, Learner satisfaction, Learner knowledge skills and attitudes, Application of learning after the program, Impact of application of learning and program characteristics associated with outcomes.	Worthwhile of a program for continuation.	Any Program.
Pre-Training ROI Calculator	Not available	Direct input from the firm's competencies, the potential candidate's past appraisal forms, training need identification and personal development plan., It reduced unnecessary expenditure and Ease the decision making process for training department.	Measure the potential return on training before and employee can be nominated for a training program	Pre-Program
Paul Kearn's Three-box model	Kearn's (2005)	Box 1: Must have Box 2: Added Value Box 3: Nice to Have	For classifying different ROI of training programs. Extension of Kirkpatrick's model. To check level of organization's commitment towards learning.	Pre-Training

3.8 PROGRAM EVALUATION MODELS AGAINST IDENTIFIED ASSESSMENT CRITERIAS.

This section briefly discusses the selected program evaluation model used in this study. As mentioned in the previous section, Kirkpatrick's Four Learning Evaluation Model is selected in this study. The discussion in this section was made on the basis of comparing the 16 identified program evaluation models (refer to Table 3.4) against the identified assessment criteria's (refer to Table 3.2).

Each of the identified program evaluation models were examined against the identified assessment criteria's as presented in section 3.5 which are attention, relevance, confidence, satisfaction, learning (context, culture and activity), attitude, subjective norms, behavioural intention and behaviour. These assessments criteria's were used to determine the most suitable model to be used in this study by examining the program evaluation assessment component, its aims and suitability. Beside the assessment criteria's the following aspect also included during the examination of suitable program evaluation models; i) the ability of the program evaluation model to assess youngsters ii) to provide improvement to the current module of the cybersecurity awareness program and finally iii) its suitability to assess youngsters and gain their feedback as desired. Basically the purpose of this comparison is to ensure only suitable program evaluation model is selected in proposing a conceptual framework to be employed. In the early comparison stage, the objectives of each model is examined and the model that found to have specific assessment focus such as on legal, art, costing, intervention and phenomenology were not suitable. Among the valid

model are Kirkpatrick Four Learning Evaluation Model, Theory Based Evaluation Model, Transaction Model, Goal Free Evaluation Model, CIPP Model and Cervero's Continuing Education Evaluation Model. However out of these models only two models found suitable for assessing motivation, which are learning and behaviour as suggested in the assessment criteria. Upon examination, this study nominated Kirkpatrick's Four Learning Evaluation Model for developing its conceptual framework. This is due to its practicality to assess youngsters, simplicity in terms of non-confusing components used, and suitability of the program because the cybersecurity awareness program is considered a training program. The following paragraph explains the fully comparisons made among program evaluation models against the identified assessment criteria's.

This study is meant to capture motivation, learning, attitude and behaviour of the youngsters' after attending the cybersecurity awareness program. It consists of combination of quantitative and qualitative methods. In comparison to Theory Based Evaluation which is based on the assumption of elements for a program to be considered successful, this study required predetermined components which were suitable in assessing a program, as in Kirkpatrick's model, the four level of evaluation is clearly determined. The four levels are reaction, learning, behaviour and impact which are found to be related with the identified assessment criteria's. Furthermore, this study used a mixed-methods approach which provides multiple data collection based on the components being studied. As compared to Experimental and Quasi experimental design, these models are not suitable to be used in this study because they are only concerned between independent and dependent variable relationship which are normally found in a quantitative approach. From the

observed phenomenon perspective, this study does not involve any sequential assessment of developmental stages as proposed by the Discrepancy Evaluation Model which is more focused on evaluating the program starting from its design, input, output and cost. With regard to the cost, this study does not involve calculation/determination of cost effectiveness as in program evaluation models such as the Discrepancy Evaluation Model, Systematic Evaluation, Pre-Training ROI Model and Paul Kearn's Three-box Model. Certain program evaluation models were customised to assess specific fields such as Responsive Evaluation, Connoisseurship Evaluation, Quasi-Legal Approach and Art Criticism Model, thus making it inapplicable for this study. For instance, the Quasi-Legal approach is specifically used in the evaluation of hearing cases in court. The Art Criticism Model and Connoisseurship Evaluation are more appropriate to evaluate something that is more subjective such as document or art artefacts. This study has a specific objective, which is to determine whether the current cybersecurity awareness program is effective in delivering its message on personal data protection. Therefore, the goal-free evaluation is not suitable for this study because it has a predetermined objective as opposed to a goal-free evaluation model which contains no objective as claimed to avoid biasness. This study is based on one assessment and does not involve multiple assessments, thus making the Transaction Model not suitable for the nature of this study. Moreover, this study does not focus on continuation of training program because its purpose is to make improvements to the program based on the identified output. The program evaluation technique that can be used to determine the commitment is Paul Kearn's Three-Box Model and Cervero's Continuing Education Evaluation.

The best evaluation models fits the assessment criteria's for this study are the CIPP Evaluation Model and Kirkpatrick's Four Learning Evaluation Model. However, due to the nature of this study that focuses on the learner-related and behavioural instead of outcomes elements, Kirkpatrick's Four Learning Model is more appropriate. The justifications for selecting Kirkpatrick's Four Learning Evaluation Model are briefly discussed in the next section.

3.8.1 Kirkpatrick's Four Learning Evaluation Components

The four learning evaluation model was introduced by Donald Kirkpatrick in 1975 as a way to evaluate a program (Kirkpatrick, 1994). Kirkpatrick's Four Learning Evaluation Model consists of four levels of evaluation namely Level 1 – Reaction, Level 2- Learning, Level 3- Behaviour and Level 4 – Results as depicted in Figure 3.5. The evaluation procedure of using this model is conducted step by step. The valuable information is gathered from all level of assessments and the findings were merged.

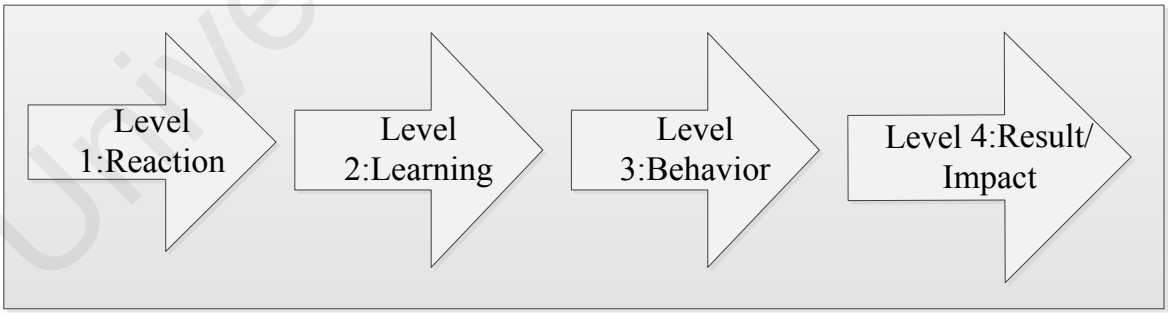

Figure 3.5: Kirkpatrick Four Learning Evaluation Model

There are different reasons for program evaluation selection. According to Kirkpatrick (1994), the specific aims could be to justify the contribution of a particular training, decision making purpose on continuation or discontinuation and for making improvement to a program. In this research, the Kirkpatrick's Four Learning Evaluation Model is used to make improvement to the current state of the cybersecurity awareness program. The assessment in this study is conducted after the program, by utilising several methods of collecting information pertaining to reaction, learning, behaviour and impact of the program. The target of this study is to propose a framework through the application of program evaluation model and employ it in assessing cybersecurity awareness program among youngsters. Thus, the mixed methodology used in collecting information from the participants starts with quantitative and followed by qualitative methodologies. The details of the research methodology are explained in the next chapter.

3.8.1.1 Level 1 – Reaction

The assessment of reaction is defined as to identify the participant reaction or motivation towards the program content. The general rules of reaction assessment are that it must ensure that participant acts favourably towards the program content which would then motivate them to learn more. Kirkpatrick (1994) underlined several reasons for measuring reaction which are: (a) To provide beneficial feedback, comments and suggestion for program improvement. (b) To assess the credibility of program coordinator and (c) as a way to provide quantitative measurement for the program stakeholders. Lastly, (d) facilitate the program standards outline for future programs. In the context of this study, assessment

of reaction is meant to identify the general view of participants who attended the cybersecurity awareness program with regard to the program content, understanding the concept of personal data protection, as well as the effectiveness of the methodology used to convey the security awareness message.

3.8.1.2 Level 2- Learning

The assessment of learning among participants is composed of three branches which are (a) knowledge, (b) skills and (c) attitudes. The importance of having this assessment level is that it stands as a predecessor for the next assessment on behaviour. This is due to the fact that there must be changes in either one of the three branches listed above to have a considerable effect on changing the behaviour. In the context of this study, participants are expected to gain knowledge on security threats, understanding few actions to be taken while dealing with security threats and having a positive attitude in keeping personal information while engaging in online activities.

3.8.1.3 Level 3- Behaviour

The third assessment level is more complicated due to the fact that the measurement of knowledge transfer from the previous level is determined in this stage. The measurement of behaviour is subjective and varies to each individual. Therefore, in the context of this study, the assessment of behaviour takes place in a special by observing and recording the participants' activities while engaging in online activities. Behavioural changes are a

complex processes and often requires longer time frame to observe whether changes have occurred. This study was conducted based on two cybersecurity awareness programs only and time was limited for behaviour observation. Therefore, in order to justify the behavioural change, the data was collected using other methodologies such as surveys, pre and post-test surveys and interviews. The recorded observation data was compared against other data collected and determination was made whether the observed behaviour is real.

3.8.1.4 Level 4- Result

This is the final assessment level which informs on the quality of the cybersecurity awareness program. The determination of quality is the most difficult part of the assessment. However, it can be shown by analysing the data collected in the previous level and later verified by a focus group interview. The actual change in behaviour determines whether the cybersecurity awareness program had met its objectives.

3.9 PREVIOUS STUDIES THAT USED KIRKPATRICK'S FOUR LEARNING EVALUATION MODEL

Although it was introduced back in 1975, the use of Kirkpatrick's Four Learning Evaluation Models is still applicable for current research. Few studies were examined to justify the practicality for this study (please refer to Table 3.5). The review articles were derived from the medical, information technology, human resource management, and retail organization and education fields. In recent years Grzeskowiak et al. (2015), Rafiq (2015)

and Tan & Newman (2013) used Kirkpatrick's Four Learning Evaluation Model as a way to perform their systematic literature review (SLR). The new extended usage of Kirkpatrick's Four Learning Evaluation Model allowed the assessment study to identify whether it consists of multiple component of evaluation as proposed by Kirkpatrick's Four Learning Evaluation Model or for only selected elements. It was identified by both Grzeskowiak et al. (2015) and Rafiq (2015) that most studies focused on Level 1 and 2 only. Level 3 and 4 were neglected. This was also applicable to the study done by van den Eertwegh et al., (2013). In the study made by Yardley & Dornan (2012) in determining the suitability and practicality of Kirkpatrick's Four Learning Evaluation Model in application as measuring tool in the medical education field, it was concluded that Kirkpatrick's Four Learning Evaluation Model has strong ability to provide evidence and the outcome was easy. However, the program assessed must be relatively simple in instructional designs, short-term program and modeled to be beneficiaries other than targeted to become learners which normally involve a very long process. Hogan, Cepela, & Fentress (2014) used Kirkpatrick's Four Learning Evaluation Model as a basis to address challenges in evaluating training by incorporating technology as assisted tools. In relation to the Information Technology field, Kirkpatrick's Four Learning Evaluation Model has been used to measure the effectiveness of e-learning programs as in Chenwo (2012), where four components were used thus justifying the usage of Kirkpatrick's Four Learning Evaluation Model in evaluating information technology programs. Rafiq (2015) used Kirkpatrick's Four Learning Evaluation Model in a human resource training to assess the effectiveness and identified that Kirkpatrick's Four Learning Evaluation Model meet the requirement and was justified for an assessment at individual level. This is the best model to select when it

comes to simplifying the complexity of the program. Moreover, through the literature search, few identified studies that use Kirkpatrick's Four Learning Evaluation Models selected it for the reason of finding the purpose of evaluation and how the assessment in each level was conducted. Kirkpatrick's Four Learning Evaluation Model is flexible enough to be used in any field. The flexibility of this assessment model also gives an advantage for this study to select the methodologies in collecting evidence or data. Thus, this study aims to use mixed methodologies by combining quantitative and qualitative research methodologies to gather evidence and carry out the analysis. The details of the selected methodologies are presented in the next chapter. In addition, in review article of Bates (2004), critical analysis using Kirkpatrick's Four Learning Evaluation Model was performed. To his judgment, although the model had aged it was still popular up to present context because of its systematic procedure and understanding of the need of evaluators. The distinct components used for evaluation has made Kirkpatrick's Four Learning Evaluation Model able to simplify the complex programs being presented to the audience. Immediate response has also added to the popularity of this model as an evaluation technique because it allows presentation of a collection of responses right after the evaluated program completed. Kirkpatrick's Four Learning Evaluation Model does not perform pre-training evaluation, or any evaluation during the overall training session. Through this model, evaluation is done just after the overall training session is completed. Each feedback from the audience is considered important. Thus it is justified that Kirkpatrick's Four Learning Evaluation Model is selected as a model to construct a conceptual framework for this study.

Table 3.5: Previous Studies applying Kirkpatrick's Four Learning Evaluation Model

Authors	Purpose of study	Assessment on Reaction	Assessment on Learning	Assessment on Behavior	Assessment on Result
Grzeskowiak, Alicia E. Thomas, Alicia E. To, Phillips, & Reeve (2015)	Examines the effect of incorporating clickers within practice-based education sessions on educational outcomes of health care trainees and professionals	Literature search			
Rafiq (2015)	Evaluating training effectiveness at airline organization	Interview			
Tan and Newman (2013)	Evaluating sale force training	Survey			
van den Eertwegh, van Dulmen, van Dalen, Scherpbier, & van der Vleuten (2013)	To reduce the inconsistencies of findings and the apparent low transfer of communication skills from training to medical practice	Literature search			
Yardley and Dornan (2012)	To explore alternative ways of appraising research evidence	Narrative literature review, a critical review of theory and qualitative empirical analysis, conducted within a process of cooperative inquiry.			
Chenwo (2012)	E-learning effectiveness	Interview	Practical operation	Observation	Observation
Farjad (2012)	Identifying the effectiveness level of job-based at higher education	Survey			
Chang (2010)	Assessing the sales training program perform at the hospitality industry.	Scoring checklist			
Praslova (2010)	Identifying the effectiveness level of learning outcomes at higher education.	Instrument that capable to measure instruction. Survey	Pre-test and post test	Conducted at the end of the program. Document analysis and observation	Conducted at the end of the program. Document analysis, survey and observation.
Caetano (2007)	Analyzing the mediating effects of perception of learning between occupational satisfaction, affective reactions, utility reactions and perceived training transfer. This study only covers assessment on reaction and learning.	Survey		Not Applicable. This study only focuses assessment of reaction and learning.	
Busch, O'Brien, & Spangler (2005)	Assessing the leadership quality and quantity via various methodologies.	Survey		Observation, Document analysis and interview	Survey

3.10 THE DESIGN OF CONCEPTUAL FRAMEWORK

In the process of designing the conceptual framework, there were 5 steps involved as illustrated in Figure 3.6. These steps were taken to ensure the valid construct and groundwork for the conceptual framework is developed. The first step is the identification of suitable theories to stand as the groundwork that provides prescription to find assessment criteria's that used to nominate suitable program evaluation model as mentioned ealier in this chapter. The identification of suitable theories has discovered ARCS Model, SLT and TRA as appropriate theories to support this study. Among the suggested assessment criteria's are motivation that refers to the positive reaction to sustain attention and favourability, learning that compose of acquisition of knowledge, skills as well as attitude, behaviour explains by act of individual towards somethind and finally attitude which influence actual behaviour.

In step 2, all these four identified assessment criteria's were further used to nominate program evaluation model. As mentioned in the previous section 3.7, program evaluation models are varies and have it own aims and suitability. Therefore in order to ensure valid selection of program evaluation model in this study, the four assessments criteria's were used in making comparison among the available program evaluation model as discussed in the previous section 3.8. Based on the comparison, the selected program evaluation model was Kirkpatrick Four Learning Evaluation. It was nominated as the appropriate model that suits the identified assessment criteria and this assist to construct the conceptual model proposed in this study.

In the early discussion of this thesis, there were three identified components of personal data protection which are password management, ii) the usage of social technologies and iii) concerns over privacy. These components were derived based on the literature review conducted. Thus in step 3, all these components were incorporated into the Kirkpatrick Four Learning Evaluation Components which are reaction, learning, behaviour and result (attitude). The purpose of this step in to make sure the tested items in the instruments later focus particularly on personal data protection as it is the main concern of this study.

In step 4, the combination of components from Kirkpatrick Four learning Evaluation Model and personal data protected has lead to the design of conceptual framework presented in the next section. Finally in step 5, the conceptual framework is practically tested for verification and validation through four sequential phases of data collection. The details of four phases are discussed in the next chapter.

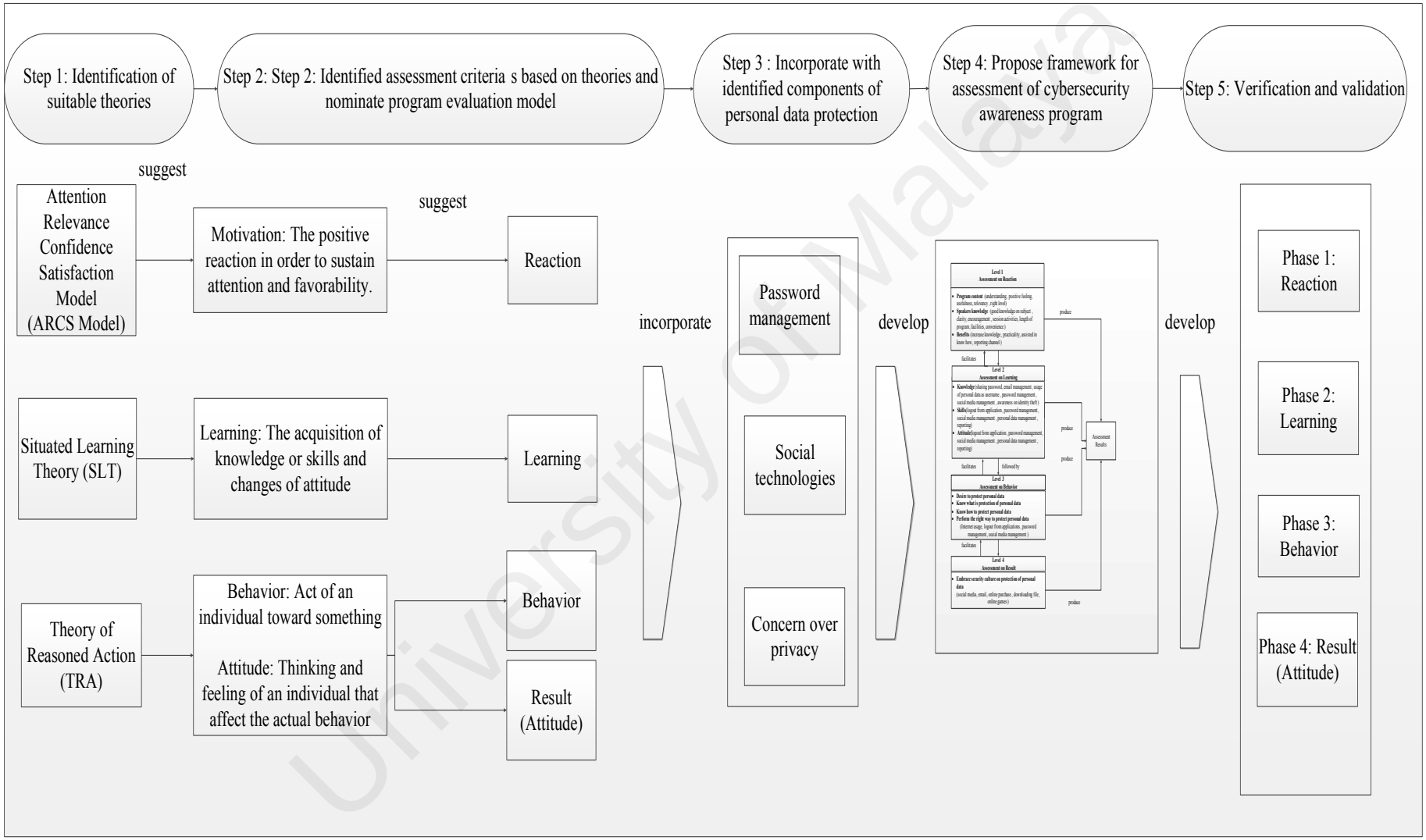

Figure 3.6: Summary of Process to Derive the Conceptual Framework

3.11 CONCEPTUAL FRAMEWORK

It is important to assess the cybersecurity awareness program on personal data among youngsters to ensure the current method of conveying messages on personal data protection is effective and well understood by youngsters. Cybersecurity awareness programs are a necessary effort made by the Malaysian government to educate and as a platform to remind to youngsters regarding the importance personal data protection while taking part in Internet activities. This is to ensure that the youngsters are well equipped with knowledge, skills and the desired attitude in any cases should they encounter any cyber threats that involve illegal use of personal data. Thus, a conceptual framework for the assessment of the cybersecurity awareness program was constructed based on the findings from the literature reviews and relevant programs evaluation models discussed earlier. This will guide the researchers and provide a clear picture of the research. The framework is a system to justify the understanding level of youngsters, key variables and theories that support the research. Figure 3.6 shows the conceptual framework for this research.

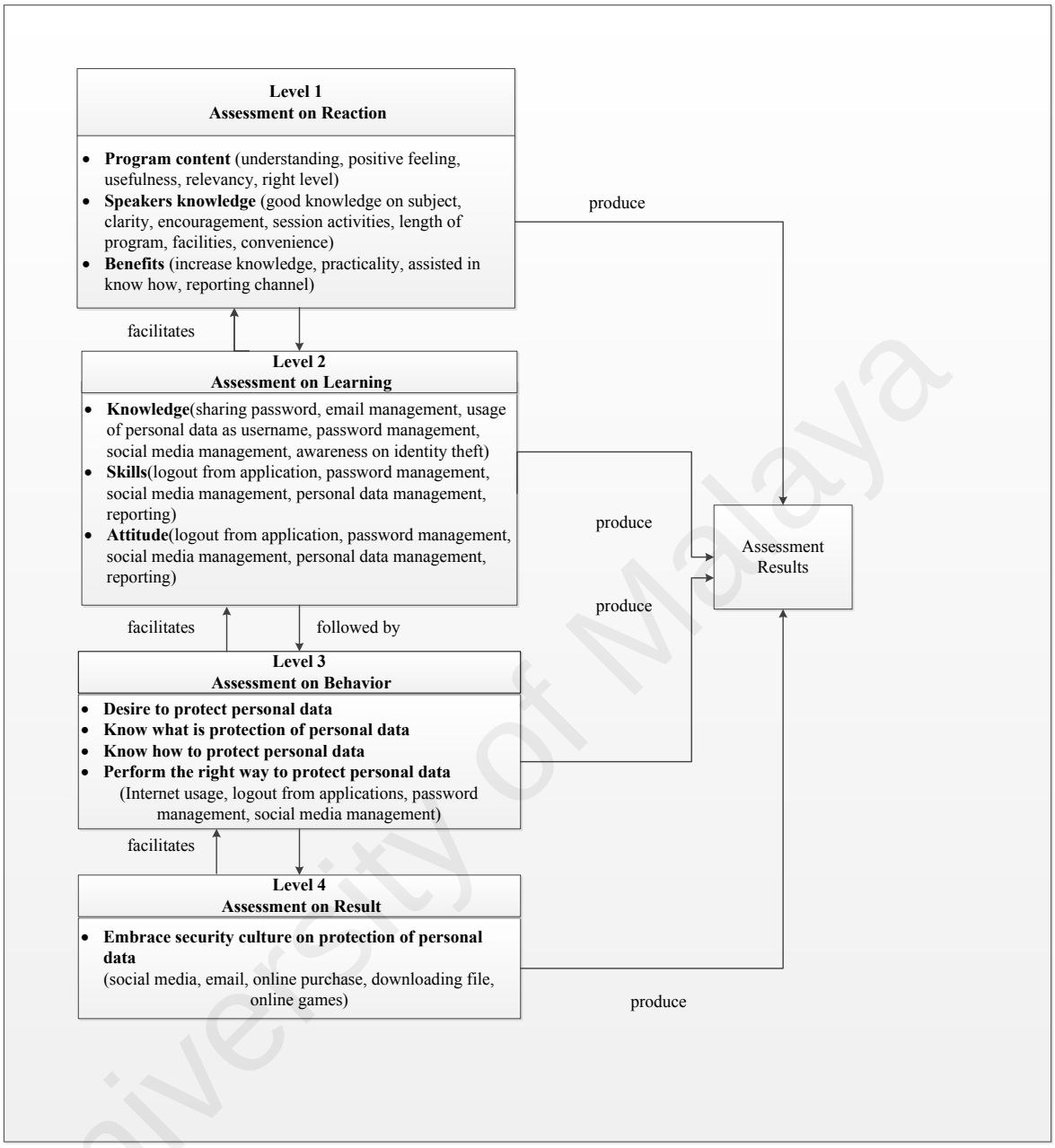

Figure 3.7: Conceptual Framework for an Assessment of Cyber Security Awareness Program

This framework depicts major levels adapted from Kirkpatrick's Four Learning Evaluation Model; Level 1- Reaction, Level 2- Learning, Level 3- Behaviour and Level 4- Result.

These levels are later translated into steps in performing data collection. Basically, the assessment of the cybersecurity awareness program is conducted step by step which careful examination of the feedback gathered from the attended participants of the cybersecurity awareness program. This framework is developed to answer the research question on i) What are the identified assessment criteria's for cybersecurity awareness program based on program evaluation model and component of personal data protection? and ii) What is the proposed assessment framework for cybersecurity awareness program?

The construct for developing this conceptual framework is basically based on the i) four level of Kirkpatrick Four Learning Evaluation Model (refer to subsection 3.4.1 and ii) component of personal data protection (refer to subsection 2.3.1). The next paragraph provides brief explanation on the overall construct of conceptual framework.

Level 1- assessment on reaction involves three sub categories of assessments which are assessment towards the program content, features and benefit. The elements for assessment on reaction are derived from the original model proposed by Kirkpatrick (1975). Level 2- assessment on the level of change in learning which involves sub-assessments on knowledge, skills and attitude. For knowledge, the elements on personal data protection were examined through questions development based on passwords sharing, email management, usage of personal data such as username, password management, social media management, awareness on identity theft. Meanwhile, for skills and attitude, elements on personal data protection were asked based on logout from application, password management, social media management, personal data management and

reporting. For each level presented in the conceptual framework, there are elements that involve personal data protection. For Level 3 assessment on behaviour, the assessment was based on the desire to protect personal data, knowing what protection of personal data is, knowing how to protect personal data and performing the right way to protect personal data. This involves the observation of the following: Internet usage, logout from applications, password management, and social media management. The final level is Level 4, which is assessment on result, includes an examination on how the youngsters embrace the security culture on protection of personal data (social media, email, online purchase, downloading file and online games).

3.12 ¶CHAPTER SUMMARY

This chapter discussed the underlying theories and concepts used in designing this research. In particular, the use of ARCS Model of Motivational Theory, Situated Learning Theory and Theory of Reasoned Action. Based upon a synthesis of the constructs in the theories, program evaluation model and the concepts from the literature, a conceptual model is proposed to be used in the research design. In addition this chapter also discussed the program evaluation models and how to use it in this study. In particular, the literature review also covered on Kirkpatrick's Four Learning Evaluation Model, which was used in constructing the conceptual framework of this research study. Each component in Kirkpatrick's Four Learning Model was briefly discussed.

The following chapter discusses the research methodology in detail starting with research paradigm, research processes involved, research approaches, research design, data

collection instruments, population and sampling, research trustworthiness as well as validity and reliability concept

CHAPTER 4

RESEARCH METHODOLOGY

4.1 INTRODUCTION

This chapter outlines the research paradigm, selection of research methodology and how Sequential Explanatory Design is applied as mixed method approach in this study. This chapter also covers the research setting selection of research samples, research instruments, and data analysis techniques. The research methodology for this study involved four sequential mixed method instruments namely; survey, pre-test and post-test surveys, interview and observation of web recording. The concept of mixed method research methodology is explained briefly in the research approach section. This is followed by an explanation of the research instruments development and the validation processes involved for the instruments used. The primary objective of this study is to propose an assessment framework for assessing cybersecurity awareness programs. Thus the instruments were constructed based on the proposed conceptual framework to fulfil the said objective. Finally, this chapter also discusses the trustworthiness of this research by focusing on the reliability, validity and quality of the collected data.

4.2 RESEARCH PHILOSOPHY

Research philosophy is an important element to determine prior a research is conducted because it influences the practice of research and methodology used (Creswell, 2009; Mingers & Brocklesby, 1997). Some scholars denoted research philosophy as research

paradigm (Lincoln & Guba, 2000; Mertens, 1998). Research paradigm will be used to discuss research philosophy in this section. According to Mackenzie & Knipe (2006), research process must be started by selecting a research paradigm which later drives in selecting appropriate research design, selecting strategies of inquiry and data analysis. In general, there are four common research paradigms in literatures (Pather & Remenyi, 2004; Creswell, Clark, Plano L., Gutmann, & Hanson, 2003; Klein & Myers, 1999).

i) **Positivism:** Assumption that the social world can be studied in the same way scientists are doing research about the natural world. It normally embarks on the theory testing concept which assists the researcher to explain the causal relationship via quantitative method.

ii) **Interpretivist:** Assumption that the reality is derived from the human experience, views and social construct. It is a normal theory building concept whereby the researcher is able to propose a theory via the qualitative method.

iii) **Transformative:** Assumption that the way of conducting research shall not be dominant to a particular method, whether quantitative or qualitative. This paradigm is appropriate for use in research related to social injustice and marginalised people as well as in politics or political agenda. It is normally conducted by combining the quantitative and qualitative methods.

iv) **Pragmatic:** Assumption that no loyalty concept shall be applied to any paradigm as it allows both methodologies, quantitative and qualitative, to be used together in the form of a mixed-method research design.

This study suggested pragmatic as a research paradigm to guide the whole process of the assessment of the cybersecurity awareness program. Pragmatic worldview is derived from a philosophical view of seeing the world in terms of actions, situations and its consequences rather than just empirical observation as in post positivism (Creswell, 2009). Mertens (2005) mentioned that pragmatic is suitable for studying the social phenomenon as compared to experimental design which suits the nature of this research which studies a phenomenon involving youngsters as a social group. Pragmatic is not committed to any particular philosophy because the direction for this worldview derived from the formulation of research question on "what" and "how" basis. This allows an in-depth analysis and description being made (Mackenzie & Knipe, 2006). The formulation of the research questions in the earlier chapter of this thesis was based on "what" and "how" thus advocates the selection of pragmatic as the research paradigm. This study was conducted via pluralistic approach through a combination of mixed data collection techniques which makes it suitable to apply pragmatic approach as the selected research paradigm. This is because pragmatic is commonly found in mixed method research (Mertens, 2014; Somekh & Lewin, 2005; Tashakkori & Teddlie, 2003). However, it is an important notation in pragmatic paradigm, a philosophical framework or theory is required to support the study.

4.3 RESEARCH APPROACH

The normal practice in research uses a single method approach as a way to perform a research (Patton, 1990). However, for better results and findings, a mixed method approach is often used in conducting a research (Neuman, 2002; Mugenda, 1999; Hansen, Cottlr, Negrine, & Newbold, 1998). This study used the mixed method approach by mixing data

collected through quantitative and qualitative methodology. This strategy was used in order to capture the details of situations that were being studied by allowing the qualitative and quantitative method to complement each other and provide robust analysis (Creswell, 2009).

In order to achieve better result and findings, this research adopted surveys, pre-test and post-test surveys, interviews and observation of web recordings as a way to assess the cybersecurity awareness program conducted by Cybersecurity Malaysia.

4.3.1 Mixed Method

There were three main research methodologies used by researchers, purely quantitative, qualitative or a mixture of both methodologies. This study used a mixture of both methodologies, which is also known as mixed method research methodology as a strategy for single research inquiry (Venkatesh, Brown, & Bala, 2013). According to Johnson & Onwuegbuzie (2004), the mixed method research methodology is carried out in order to have better understanding, explain or build on the result of a phenomenon of interest. Also mentioned by Creswell (2009), the data collected through the mixed method procedure can minimise biasness as compared to a single method because it could neutralise the finding by having multiple instruments used for data collection. Venkatesh et al. (2013) support the use of the mixed method by suggesting that utilising the mixed method strategy could assist Information System (IS) researchers in making contribution to theory and practice.

This method do not meant to replace either a quantitative or qualitative methodology, but rather to combine their strengths and weaknesses to form constructive findings from a research (Johnson & Onwuegbuzie, 2004). Usage of the mixed method research in program evaluation research is not new as Greene, Caracelli, & Graham (1989) highlighted that program evaluation has benefited from the mixed method research methodology. In program evaluation study, the mixed methodology has been widely adopted by evaluators of social and educational programs. It terms of its purpose, there are five possibilities of purposes which are triangulation, complementary, development, initiation, and expansion (Creswell, 2009; Creswell et al., 2003) as shown in Table 4.1.

Table 4.1: Purpose and Rational to Adopt Mixed Method Strategy for Evaluation Design (Greene et al., 1989)

Purpose	Rationale
TRIANGULATION seeks convergence, corroboration, correspondence of result from different methods.	To increase the validity of constructs and inquiry results by counteracting or maximizing the heterogeneity of irrelevant sources of variance attributable especially to inherent method bias but also to inquirer bias, bias of substantive theory, biases of inquiry context.
COMPLEMENTARY seeks elaboration, enhancement, illustration, clarification of the results from one method with the results from other method	To increase the interpretability, meaningfulness and validity of constructs and inquiry results by both capitalizing on inherent method strengths and counteracting inherent biases in methods and other sources.
DEVELOPMENT seeks to use the results from one method to help develop or inform the other method, where development is broadly construed to include sampling and implementation, as well as measurement decisions.	To increase the validity of constructs and inquiry results by capitalizing on inherent methods strengths.
INITIATION seeks the discovery of paradox and contradiction, new perspectives of frameworks, the recasting of questions or results from one method with questions or results from the other method.	To increase the breadth and depth of inquiry results and interpretations by analyzing them from the different perspectives of different methods and paradigms.
EXPANSION seeks to extend the breadth and range on inquiry by using different methods for different inquiry components.	To increase the scope of inquiry by selecting the methods most appropriate for multiple inquiry components.

This study used the mixed method research methodology for the purpose of complementary. The clarity of findings could be explained from one method with the findings from other methods. This helps to increase the interpretability and meaningfulness of findings. Because of the above mentioned purpose, this study applied the mixed method strategy for realisation through data collection technique. According to Creswell (2009), six different types of mixed method strategies were available as presented in Table 4.2. The implementation of the mixed method research methodology was based on the suitable strategy as suggested by Creswell (2009).

Table 4.2: Mixed Method Strategies (Adaptation from Creswell, 2009)

Category	Mixed method strategy	Steps	Criteria	Advantages	Disadvantages
Sequential	Sequential Explanatory Design	Started with quantitative data collection followed by its analysis. The next step involves qualitative data collection and its analysis. The result will be based on the entire analysis.	Weight is given to quantitative data collection and its analysis Quantitative data informs the qualitative data Qualitative data used to interpret the quantitative data Able to capture unexpected result Theoretical perspective is not mandatory	Straightforward Steps are clear and separated Assist to provide easier report and findings	Longer time frame to complete both data collection.
	Sequential Explonatory Design	Start with qualitative data collection followed by its analysis. The next step involves quantitative data collection and its analysis. The result will be based on the entire analysis.	Reverse of Sequential Explanatory Design Qualitative data will build upon quantitative data. Weight is given to qualitative data collection and its analysis Theoretical perspective is not mandatory Used to explore a phenomenon Assist in the case of inadequate of existing instrument	Straightforward Steps are clear and separated Assist to provide easier report and findings	Longer time frame to complete both data collection.
	Sequential Transformative Design	Quantitative or qualitative methods used either one use as the first or later. Which one use earlier will build to the next chosen method.	Explore a problem, understand a phenomenon or process that changing. Drives by theoretical perspectives as guidance through conceptual framework	Straightforward Steps are clear and separated Assist to provide easier report and findings	Longer time frame to complete both data collection.

Table 4.2 continued: Mixed Method Strategies (Adaptation from Creswell, 2009)

Category	Mixed method strategy	Steps	Criteria	Advantages	Disadvantages
Concurrent	Concurrent Triangulation Design	Quantitative and qualitative were collected simultaneously	Compare the collected data to determine the union, differences or overlapping. Used to balance the weaknesses produced by either method. Used to add strength to other method.	More familiar and produced well validated result and findings. Shorter time because both data collection technique can be done at the same time	Great expertise to study two phenomenon's at the same time. Different types of data collected were hard to analyses. Unclear ways to solve discrepancies in result.
	Concurrent Embedded Design	Identified by data collection phase. Result will cross validate and compared to each other.	The second method may have different question than a primary method. Have explicit theoretical perspective.	Gain broader perspectives Shorter time for data collection	Great amount of work required to ensure the data can be integrated with the analysis phase May create unequal result due to unequal weight of both methodologies
	Concurrent Transformative Design	Research strives by a specific theory. It has choice of model to facilitate theoretical perspectives.	Equal or unequal priority during data collection Integration of two methods normally occurs during the analysis stage.	Gain broader perspectives Shorter time for data collection	Great amount of work required to ensure the data can be integrated with the analysis phase May create unequal result due to unequal weight of both methodologies

This study apply mixed method strategy using Sequential Explanatory Design (please refer to Figure 4.1). This strategy proposes the application of quantitative or qualitative research methodology by given weight to quantitative data collection and its analysis. In this study, the steps for using sequential explanatory design were conducted in sequence labelled as phase. The first and second phases involved quantitative data and followed by qualitative data collection for the third and fourth phase. The result in this study is based on the entire analysis. Even though theoretical perspectives is not mandatory for this mixed method strategy, the establishment of theoretical perspectives in the form of conceptual framework is still applicable to this study. This is due to the reason that the conceptual framework acts as a theoretical in shaping the direction of the research (Creswell, 2009; Creswell et al., 2003). Thus, report of the findings and integrating it will be made easier. However, the disadvantage of this technique is that it requires extra amount of time and effort to conduct a sequential data collection. It also requires extra time to construct different types of instruments to be used in different phases of the data collection.

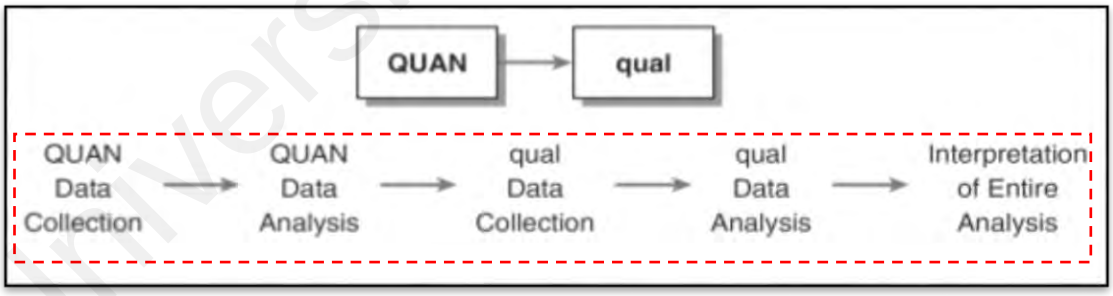

Figure 4.1: Sequential Explanatory Design Adaptation from Creswell, 2009

Instruments for the quantitative and qualitative data collection technique were constructed separately as it measure different components of one phenomenon. There were four instruments developed which were surveys for assessment on reaction, pre-test and post-test surveys for assessment on learning, observation of web recordings for

assessment on behaviour and interviews for assessment on result. The summary of the Sequential Explanatory Design used in this study is presented as in Figure 4.2.

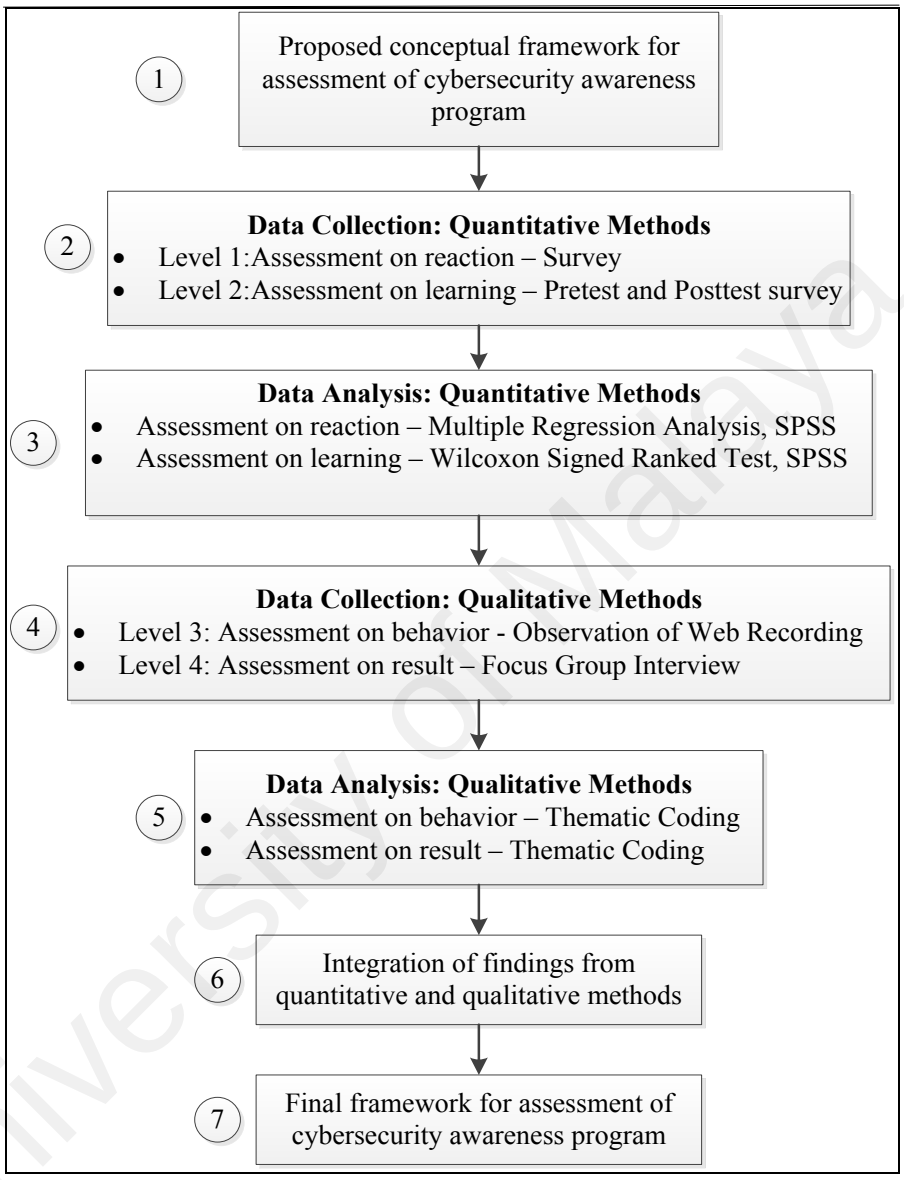

Figure 4.2: How Sequential Explanatory Design is used in this Study

Figure 4.2 depicts clear steps in executing Sequential Explanatory Design in this study. The first step is to propose a conceptual framework that guides the data collection process and its analysis. As depicted in step 2 and 4 there are four different data collection techniques used in this study. Both quantitative and qualitative techniques were used. In specific term for the assessment on reaction, surveyed is used. Meanwhile

for assessment on learning, pre-test and post-test survey is used. Both are quantitative methods. For assessment of behaviour, the observation of web recording was used and lastly for assessment of result, focus group interview was used. The assessments were conducted in sequence which means it is started by assessment on reaction, followed by learning, behaviour and finally result. As the data collection method varies, the data analysis steps also differ. In step 2, the first process is to analyse data collected for assessment on reaction by using Multiple Regression. The second process is to analyse the data collected for an assessment of learning using Wilcoxon Signed Rank Test. Step 5 involves data analysis for assessment on behaviour and result. Both were analysed separately using thematic coding. The first process of qualitative data analysis is for data collected through observation of web recording and followed by focus group interview. In step 6, the interpretation of data is made by combining all the result gathered from the four types of data analyses technique used. The finding is discussed in detail in Chapter 5. After data collection and data analysis, the final framework for assessing cybersecurity awareness program is proposed. It is an important notation that assessment conducted in this study is in the form of collective findings and gender is not an influence factor. This notation is aligned with Willingham & Cole (2013), who emphasize on fair assessment among different gender. He also suggested valid assessment shall comprise from a broad view of participants.

4.4 RESEARCH DESIGN

The research design for data collection and data analysis involves four phases. Each phase began separately but was kept in sequence. Prior to engaging in real research setting, a pilot study was conducted in April 2015 to test the instruments using real participants, and any required modification on the instruments was documented. In an actual research setting, Phase 1 is meant for assessment on reaction, Phase 2 is meant

for assessment on learning, Phase 3 is meant for assessment on behaviour and finally Phase 4 is meant for assessment on result. Data collections were held at two OUTREACH CyberSAFE programs conducted by Cybersecurity Malaysia. First program was held at Bahagian Teknologi Pendidikan Negeri Johor on 10th August 2016 which involved youngsters from all over Malaysia, referred to as Cohort 1, and the second program was held at Sekolah Seri Puteri Kuala Lumpur on 2nd September 2016 which involved only youngsters who studied in this particular school referred to as Cohort 2. Data collection for the quantitative method involved cohort 1 and cohort 2 while data collection for the qualitative method involved only participants from cohort 1. For the purpose of qualitative analysis only 12 participants involved from Cohort 1. Therefore to achieve saturation it was first done by examine the background of participants. Even there were from Cohort 1 only, the 12 participants came from all over state in Malaysia. This is because cybersecurity awareness program is conducted at National level which involves representative from different state. Second, by examine their feedback the saturation was achieved once the 12 youngsters provide the same feedback and it was crosschecked with one focus group to the other.

Data collected from each phase was analysed separately from other phases. The technique of analysis used for analysing the quantitative data was the Statistical Package for Social Sciences (SPSS), while thematic analysis was used to analyse qualitative data. The summary of the research design for data collection and analysis is presented in Table 4.3. The details of each phase are discussed in subsequent sections.

Table 4.3: Summary of Data Collection and Data Analysis Phases

Component	Pilot study	Phase 1	Phase 2	Phase 3	Phase 4
Instrument	Closed-ended survey, pre-test and post-test survey, Observation of web recording checklist, Focus group interview protocol	Closed-ended survey	Pre-test and Post-test closed ended survey	Observation of web recording checklist	Focus group interview protocol
Sampling type	Convenience sampling			Focus group (purposive sampling)	
Participants/respondent (youngsters attended program)	50	384	Pre-test: 397 Post-test: 391	12 (same pool of youngsters)	
Data Analysis	Multiple Regression	Wilcoxon Signed Rank Test		Thematic Analysis	
Date	4th April 2015	10th Aug & 2nd Sept 2015		10th Aug 2015	
Venue	Maktab Rendah Sains Mara Kulim	Bahagian Teknologi Pendidikan Negeri Johor & Sekolah Seri Puteri Kuala Lumpur		Bahagian Teknologi Pendidikan Negeri Johor	
Expected outcome	The suitability of instruments	The favorability of youngsters towards cybersecurity awareness program	The learning changes in term og knowledge, skill and attitude	The actual behaviour of youngsters after attending cybersecurity awareness program	The feedback by youngssters after attending cybersecurity awareness program

4.5 POPULATION AND SAMPLING FOR PHASE 1 AND 2

The unit of analysis was youngsters' age from 12-19 years old who attended the cybersecurity awareness program conducted by Cybersecurity Malaysia. For Phase 1, assessment on reaction, a total of 384 youngsters participated in answering the survey. Meanwhile for Phase 2, assessment on learning, a total of 397 and 391 youngsters participated in the pre-test and post-test survey respectively. G-Power analysis was used to calculate the minimum sample size required for quantitative analysis based on the total number of predictors (construct) in the instrument used as suggested by Hair, Ringle, & Sarstedt (2011) (please see Appendix H). In this study G-Power analysis is

used to determine the minimum number of sample required to run the analysis. The determination is based on the number of predictors in phase 1 and 2. The G-Power analysis was run using 20 (phase 1) and 27 (phase 2) number of predictors with the medium effect size of f^2=0.15. Based on the calculation of G-Power analysis, the recommended sample size is 222. Hence, this suggested that the number of responses collected for both Phase 1 and 2 were deemed reasonable to give a satisfactory response rate for analysis. For Phase 1 and 2, convenience sampling was used. Convenience sampling is a non-probability sampling method in which the individuals being studied in the population has an unequal chance of being selected. The participants in convenience sampling are selected from the populations that are easily accessible, available and convenient to be studied (Creswell, 2009).

4.6 POPULATION AND SAMPLING FOR PHASE 3 AND 4

The unit of analysis was the same youngsters' age from 12-19 years old who attended the cybersecurity awareness program conducted by Cybersecurity Malaysia. After completing the data collection for Phase 1 and 2, consent forms were given to the teachers as representative for guardian to nominate and suggest youngsters from different demographic backgrounds to participate in the observation of web recording and focus group interview. Consent letters for participation were required because this study involved participants aged below 18 years old (Morrow & Richards, 1996). The selected participants had the following basic criteria: i) obtain consent from the guardian or representative of guardian. ii) aged 12-19 years old. iii) attended the cybersecurity awareness program conducted by Cybersecurity Malaysia. iv) willing to respond to the findings of the interview. Since the data collection procedure involved leveraging on the cybersecurity awareness program conducted by Cybersecurity Malaysia, a letter was

prepared in order to state the intention to conduct the study. The letter stated the objective, purpose; process and procedure of data collection (please see Appendix D).

The same youngsters participated in both phases of the data collection, observation of web recording and focus group interview. The consent forms were collected from their teacher and a total of 12 youngsters were willing to participate. They were grouped into 3 focus groups with 4 youngsters per group. The use of focus groups as sampling technique is due to its wide usage in academic research to examine attitudes, feelings, experience and reaction of participants more extensively, which could not be covered by only one-to-one interviews and observation sessions (Gibbs, 1997).

The focus groups conducted in this study allowed the researcher to measure information gained from different groups of youngsters who attended the same cybersecurity awareness program conducted by Cybersecurity Malaysia. By having focus groups, it encourages youngsters to feel confident in answering, sharing and debating on relevant issues related to the questions asked by the facilitator (Reid & Reid, 2005). Furthermore, youngsters were able to react, add points to other responses and promote strategic thinking in a group setting (Kleina, Tellefsenb, & Herskovitzc, 2007). The summary of demographic profiling is presented as per Table 4.4.

Table 4.4: Demographic Profile for Observation of Web Recording and Focus Group Interview

Focus Group ID	Individual ID	Gender	Age
1	Y1	M	16
	Y2	M	14
	Y3	M	16
	Y4	M	16
2	Y5	M	17
	Y6	F	17
	Y7	M	17
	Y8	M	14
3	Y9	F	19
	Y10	M	17
	Y11	M	17
	Y12	M	17

Legend:
Y= Youngster
M = Male, F- Female

4.7 PILOT TESTING AND CONTENT RELATED EVIDENCE OF VALIDITY

The initial developed instruments (phase 1-4) were validated using a pre-testing method proposed by Cooper, Schindler, & Sun (2003) by appointing related experts who have strong background in the area of study and in trials involving real research settings. The expert review is important to ensure the validity and accuracy of items being asked during the actual data collection. In this study, two experts were appointed from two different local universities in Malaysia. The experts were academics, Dr. Nurul Nuha Abdul Molok from the International Islamic University Malaysia and Dr. Nur Jihan Abd Ghani, from the University of Malaya. The process of Content Related Evidence of Validity was first initiated by providing an official letter to both experts and seeks their cooperation to provide comments in term of the structure, continuity, relevance of content and suitability of the instruments used. After their agreement, they were given both the soft and hard copies of four different set of instruments (survey, pretest and post-test survey, observation and interview protocol) together with research objectives

and the conceptual framework for reference. Two weeks duration were given for them to perform verification and review.

The verification and review were returned in the form of hardcopy and every comment was taken to improvise the instruments. Among the highlighted concern are the term used within the instruments that might not be well understood by the participants. Both experts found the instruments suit the purpose of research objectives and followed the conceptual framework. However, there was a comment from one of the expert to provide example to the younsgters apart from the question as this help them to answer all questions accurately. Table 4.5 provides details summary of two appointed panels expert .

Table 4.5: Expert Panels Details

No	Expert name	Institution	Position	Background
1	Dr. Nurul Nuha Abdul Molok	International Islamic University Malaysia	Assistant Professor	Security system, organizational information security, social media use among employees and its impacts to organizational information security and information security management policies
2	Dr. Nur Jihan Abd Ghani	University of Malaya	Senior Lecture	Data security (personal data protection), information system security and database (security and privacy)

The revision were made to the all the instruments and sent back to experts for their endorsement. The validated instruments was tested in a pilot test on 50 youngsters who attended a cybersecurity awareness program conducted by Cybersecurity Malaysia conducted in April 2015 at Maktab Rendah Sains Mara Kulim, Kedah, Malaysia. The purpose of the pilot study was to test the constructed research instruments in a real

research setting. The findings from the pilot study and expert reviewers were merged in order to ensure each item developed was understood by participants and they could respond well. Based on the merged comments from expert reviewers and participants, any confusing items such as the concept of file sharing, encryption and online banking were deleted and only remaining survey items deemed valid were asked during the actual data collection. The deleted items were due to the participant's responds which they were not familiar with, and rarely used such as items from Internet file sharing, encryption and online banking. Beside, the findings from all instruments tested were tested using the proposed data analysis technique to ensure the result can fit the requirement of the chosen analysis technique. Among the test used for pilot study were missing value and data distributional. The missing values were revisited and it was found that participants purposedly do not answer certain questions because of the term used. The findings also were tested to meet the assumption of Multiple Regression and Wilcoxon Signed Rank Test, overall it meet the requirement for both test.

4.8 DATA COLLECTION PHASE 1 - CLOSED-ENDED SURVEY

The survey used for assessing the youngsters' reaction is close-ended items. The survey was prepared in Malay Language for better understanding among Malaysian participants. The close-ended items are suitable when a study involves participants with a similar demographic profile. The demographic profile is similar because only participants between the ages of 12 to 19 years participated in this study.

The participants were asked to respond to items asked in four sections. Section 1 contained nominal questions which were meant for demographic profiling. Section 2, 3 and 4 used the Likert scale ranging from Strongly Disagree (1), Disagree (2), Neutral (3), Agree (4) and Strongly Agree (5). A 5-point Likert scale was used to measure the

degree of favourability to each item asked. In particular, the items were meant to measure the degree of favourability to program content, quality of speaker and program benefits in relation to personal data protection. This survey was given to participants immediately after the program finished to ensure accurate answers were gathered based on their experience. (Please refer Appendix I)

4.8.1 Instrument Development

The survey consists of four sections. Section 1 is related to questions pertaining to demographic profiling. Section 2 is meant to gain feedback on the program content, Section 3 is meant to gain feedback on the program features and finally Section 4 is meant to gather information on program benefits. The structure of each section is presented as the following:

Section 1: Demographic questions such as gender, age, access to the Internet, usage of the Internet, frequency of Internet usage, attendance to any previous cybersecurity awareness program and awareness on identity theft.

Section 2: Program content such as program objective, attraction of the program, material used, relevancy, presentation and level of understanding.

Section 3: Quality of speaker such as knowledge in subject matter, clarity, example, session activity, utilisation of time, additional content required and beneficial.

Section 4: Program benefits such as increment of knowledge, practicality, know-how and reporting channel.

The type of scale used for assessment on reaction involves nominal and ordinal scale. Nominal scale is a non-overlapping scale that is used to label variables such as gender

and age. Question 1 to 7 applied the nominal scale. Meanwhile, for question 8 to 27, ordinal scales were used. Each question was assigned an identification no (ID). An ordinal scale is meant to measure non-quantifiable variables such as level of agreement as used in this study. The following Table 4.6 summarises the detail of instruments developed in term of section, label, items detail and references for assessment on reaction.

Table 4.6: The Details of Survey – for Assessment on Reaction

Section	Label	Items detail	Reference
1:Demographic	1-7	Gender, age, access to the Internet, Internet activities, hour spent and attended cybersecurity awareness and risk of identity theft.	Not applicable
2:Program contents	PC1	I understand the program objective is to educate youngsters about safety in cyber world	(Kirkpatrick, 1994; Kirkpatrick, 2009; Yardley & Dornan, 2012)
	PC2	I found this program is joyful and attractive.	
	PC3	I found the material used is useful to enhance the practice of personal data protection.	
	PC4	I found the program content is relevance for me to enhance the practice of personal data protection.	
	PC5	I felt this program has been presented at the right level to enhance the practice of personal data protection.	
	PC6	I understood the importance of protecting personal data.	
3:Program features	PPC1	The presenter has good knowledge about personal data protection.	(Kirkpatrick, 1994; Praslova, 2010)
	PPC2	The presenter has explained clearly about personal data protection.	
	PPC3	The presenter has given example about personal data protection.	
	PPC4	The presenter has encouraged the participants to have better understanding about personal data protection.	
	PPC5	I found the activities during the session help me to have better understanding about personal data protection.	
	PPC6	I found the session about personal data protection is too long.	
	PPC7	I found that session about personal data protection require additional content.	
	PPC8	I found the session about personal data protection is useful.	
4:Program benefit	PB1	My knowledge about personal data protection has increased.	(Kirkpatrick, 1994; Kirkpatrick, 2009)
	PB2	I'll practice the knowledge gained through this session to protect my personal data protection.	
	PB3	Now, I know how to protect my personal data.	
	PB4	Now, I know how to contact the responsible party if any third party ask or steal my personal data.	
	PB5	Now, I know how to act if any third party ask or steal my personal data.	
	PB6	Now, I know the importance to protect personal data protection.	

4.8.2 Data Collection Approach

Data was collected from two cohorts. Cohort 1 consists of 64 participants while Cohort 2 consists of 329 participants. Data was collected through a distribution of hardcopy surveys after the cybersecurity awareness program finished. Participants were given approximately 10 minutes to answer all items in the survey. Initially, 400 sets of surveys were distributed for both cohorts. However, only 393 participants returned the surveys. Before further analysis is conducted, the 393 gathered surveys were analysed for missing data using SPSS. 9 surveys were rejected due to incomplete answers which resulted in 384 surveys being valid for further analysis. Since the minimum sample size for this study is 222 based on G-Power calculation, thus the sample size was deemed satisfactory to fulfil the minimum number required for this study and could be used for analysis.

4.8.3 Data Analysis Approach – (Multiple Regression, SPSS)

The information in Section 1 (please refer to Table 4.6), obtained from the returned survey was coded and transferred into SPSS version 22. The coded data was in the form of numerical values in which different numbers were assigned to different answers. The descriptive analysis to determine the mean and frequency for each answer in Section 1 were used. Whilst the answer gathered from Section 2, 3 and 4 were also coded using SPSS for the future analysis using Multiple Regression. Multiple Regressions is a statistical technique that can be used to predict the relationship between dependent (criterion variable) with a set of independent (predictors variable). Underlying objective of using this technique is to find the best prediction equation for a set of variable,

identifying independent relationship by controlling confounding factors in order to assess a specific variable sets. It is also meant to find the structural relationship as similar to path analysis (Ho, 2014). There are three major categories of multiple regression, for the purpose of this analysis only standard multiple regression were used because it allows all the independent variables to be entered into the regression equation together.

4.9 DATA COLLECTION PHASE 2 - PRE-TEST AND POST-TEST CLOSE-ENDED SURVEY

The survey used for assessing participants' learning is close-ended. There are two sets of close-ended items designed for pre-test and post-test respectively. The items asked in the pre-test and post-test survey are the same. The surveys were prepared in Malay Language for better understanding among participants. The participants were asked to respond to items asked in three sections. All three sections were prepared using Likert scale ranging from Strongly Disagree (1), Disagree (2), Neutral (3), Agree (4) and Strongly Agree (5). The Likert scale is used in this assessment to measure the degree of favourability and changes to the following: knowledge, skills and attitude. Section 1 is meant to measure the level of knowledge, Section 2 is meant to measure the level of skills and finally Section 3 is meant to measure changes in attitude. Participants were given the pre-test survey 10 minutes before the program started and it is then immediately collected. The post-test survey was given right after the program ended. The analysis is based on the difference between the pre-test and post-test results.

4.9.1 Instrument Development

The survey consists of three sections as detailed in Table 4.7. Section 1 is related to questions pertaining to knowledge measurement. Section 2 is meant to measure changes in skills and Section 3 is meant to measure changes in attitude. The structure of each section is presented as the following:

Section 1: Knowledge such as management of password, management of email, management of personal identity, management of social media and risk awareness.

Section 2: Skills such as management of online application, management of password, management of social media and reporting channel.

Section 3: Attitude such as management of online application, management of password, management of online banking, management of personal identity, management of social media and reporting channel.

Table 4.7: The Details of Survey (Pre-test and Post-test) – for Assessment on Learning

Section	Label	Items detail	Reference
Section 1: Knowledge	Pre_Knowledge_1 Post_Knowledge_1	I share password with other people	(Kaye, 2011; Meter & Bauman, 2015)
	Pre_Knowledge_2 Post_Knowledge_2	I responded by replying to email who came from uknown sender	(Amanda Lenhart, 2012)
	Pre_Knowledge_3 Post_Knowledge_3	I use my fullnname as username while accessing the Internet application	(Singh et al., 2007)
	Pre_Knowledge_4 Post_Knowledge_4	I use my identification number as username while accesing the Internet application	(Singh et al., 2007)
	Pre_Knowledge_5 Post_Knowledge_5	I use the same password to access all my Internet applications	(Kaye, 2011; Singh et al., 2007; Weinstein & Selman, 2014)
	Pre_Knowledge_6 Post_Knowledge_6	I used simple password as it easy to remember	(Amanda Lenhart, 2015; Amanda Lenhart et al., 2010)
	Pre_Knowledge_7 Post_Knowledge_7	I will accept all friend request in social media application	(A Lenhart et al., 2011; Livingstone et al., 2005)
	Pre_Knowledge_8 Post_Knowledge_8	I always forget my password, therefore I wrote it in a piece of paper and paste it at computer screen	(Smahel et al., 2012; Vandoninck et al., 2014)
	Pre_Knowledge_9 Post_Knowledge_9	I made my profile public in social media	(Livingstone et al., 2005; Madden et al., 2013)
	Pre_Knowledge_10 Post_Knowledge_10	I realized the risk of identity theft and it consequences	(Chawki et al., 2015; Fire et al., 2014)

Table 4.7 continued: The Details of Survey (Pre-test and Post-test) – for Assessment on Learning

Section 2: Skill	Pre_Skill_1 Post_Skill_1	I will logout after using Internet application	(Correa et al., 2013; Amanda Lenhart et al., 2010; Madden et al., 2013)
	Pre_Skill_2 Post_Skill_2	I will change to a new password which has a combination of letter, number and symbol	(Smahel et al., 2012; Vandoninck et al., 2014)
	Pre_Skill_3 Post_Skill_3	I will not accept any friend request from unknown individual	(Livingstone et al., 2005; Madden et al., 2013)
	Pre_Skill_4 Post_Skill_4	I will not share my identification number for unknown reason	(Singh et al., 2007)
	Pre_Skill_5 Post_Skill_4	I will not share my password with other people	(Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michelle L. Mazurek, Timothy Passaro, Richard Shay, & Lujo Bauer, Nicolas Christin, 2012; Kaye, 2011)
	Pre_Skill_6 Post_Skill_6	I will have different combination of password for different Internet applications used	(Kaye, 2011; Singh et al., 2007; Weinstein & Selman, 2014)
	Pre_Skill_7 Post_Skill_7	I will change my social media setting to protect my privacy	(Livingstone et al., 2005; Madden et al., 2013)
	Pre_Skill_8 Post_Skill_8	I will report to responsible body if my personal data used by unknown individual	(Youn, 2009)
Section 3: Attitude	Pre_Attitude_1 Pre_Attitude_1	Logout after using any Internet application	(Correa et al., 2013; Amanda Lenhart et al., 2010; Madden et al., 2013)
	Pre_Attitude_2 Pre_Attitude_2	Changing your password frequently is important to protect personal data	(Smahel et al., 2012; Vandoninck et al., 2014)
	Pre_Attitude_3 Pre_Attitude_3	Filteration of friend request could avoid stealing of personal information	(Livingstone et al., 2005; Madden et al., 2013)
	Pre_Attitude_4 Pre_Attitude_4	The identification number is private and can be use for certain reason only	(Singh et al., 2007)
	Pre_Attitude_5 Pre_Attitude_5	The bank information is private and can't be given to any individual without authentic verification	(Singh et al., 2007)
	Pre_Attitude_6 Pre_Attitude_6	Sharing password is not allowed	(Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee et al., 2012; Kaye, 2011)
	Pre_Attitude_7 Pre_Attitude_7	Different password required for different Internet applications	(Kaye, 2011; Singh et al., 2007; Weinstein & Selman, 2014)
	Pre_Attitude_8 Pre_Attitude_8	Changing setting in social media application is important to protect personal data	(Livingstone et al., 2005; Madden et al., 2013)
	Pre_Attitude_9 Pre_Attitude_9	Reporting of any security breach to responsible body is important	(Youn, 2009)

4.9.2 Data Collection Approach

The same two cohorts were used for the pre-test and post-test surveys. Data was collected on the same day through a distribution of hardcopy survey before and after the program. For the pre-test survey, participants were given approximately 10 minutes to answer all items in the survey before the cybersecurity awareness program started. All answered surveys were gathered immediately after 10 minutes totalling 400 for cohort 1 and 2. Initially, 400 sets of pre-test surveys were distributed for both cohorts, and 200 sets per cohort. All 400 sets of surveys were returned because it was gathered right after the 10 minutes duration that was given. The 400 gathered surveys were initially analysed for missing data in SPSS. 3 surveys were rejected due to incomplete answer which made 397 surveys were valid for further analysis. Calculation using G-Power analysis shows that the minimum sample size is 222 based on the total predictors' number. Thus it was deemed satisfactory to fulfil the minimum number that is required for this study and could be used for analysis.

For the post-test arrangement, the participants were given approximately 10 minutes to answer all items in the survey right after the program ended. All answered surveys were gathered immediately after 10 minutes which totalled to 400 for cohort 1 and 2. As in the pre-test, all 400 surveys were returned and after the data cleaning process, a total of 391 surveys were considered clean without missing elements and could be used for analysis. The summary of the data collection strategy for both data collection procedures depicted is in Table 4.8:

Table 4.8: A Summary of Data Collection Strategy for Phase 1 and 2

Cohorts	Date	Place	Phase 1 Participants	Phase 2 Participants
Cohort 1	10th Aug 2015	BTPN (Bahagian Teknologi Pendidikan Negeri Johor), Johor	64	64
Cohort 2	2nd Sept 2015	Sekolah Seri Puteri Cyberjaya, Selangor	329	336
Minimum sample required			222	222
Total participants			393	Pre-test: 400 Post-test: 400
Total participants after removing missing value (List wise deletion)			384	Pre-test: 397 Post-test: 391

4.9.3 Data Analysis Approach- (Wilcoxon Signed Rank Test - SPSS)

Data and information obtained for all returned pre-test and post-test surveys were coded and transferred into SPSS version 22. The coded data was in the form of numerical values in which different numbers were assigned to different answers. The coded data for both the pre-test and post-test surveys initially tested for normality in SPSS and revealed as non-parametric data. Due to extreme violation of the normality assumption of pre-test and post-test data, the Wilcoxon Signed Rank Test was used to compare the signed rank test for two related samples instead of a normal related t-test (Ho, 2014). The purpose of Wilcoxon test is to measure the different between two set of data from individual. The normality assumption refers to normal distribution of the collected data. The ordinal data collected were transferred to become a group of pre-test and post-test score based on 3 sections: knowledge, skills and attitude. The assumption constructed based on the developed conceptual framework was used to measure whether youngsters had gained knowledge, increased skills and changed their attitude on personal data protection after attending the cybersecurity awareness program. Level of significance is determined by $p>0.05$ and the two-tailed test is based on critical value of z which must be within -1.96 and +1.96 (Ho, 2014).

4.10 DATA COLLECTION PHASE 3 – OBSERVATION OF WEB RECORDING

For the behaviour assessment, the observation of web recording is used as an instrument to measure the change in behaviour of participants after attending the cybersecurity awareness program. The observation of web recording was selected as a strategy of inquiry because it allows the researcher to have first-hand experience with the participants. The observation of web recording is an observation conducted to record youngsters' activities while they browsed the Internet. The observation was recorded using a tool named Camtasia Studio (please see Appendix P). The Camtasia Studio is selected as a tool to provide screen captured in the form of video. During the observation of web recording, a field note was taken to observe the scenario and recording process. As suggested by Creswell (2009), any unusual aspects can be spotted and recorded using a field note. In conducting observation of web recording, an initial observation checklist was prepared to record the participant's online activities. This study used observers who observed without participating (Creswell, 2009). Accordingly, 12 participants were observed. Prior to the observation, several tasks were required to be done. Summary of these tasks is presented as the following Table 4.9.

Table 4.9: Summary of Task for Observation of Web Recording

Research Process	Tasks	Activities
Planning	Identify the likely participants to be observed	Sent and collect the consent letter from the representative of guardian as permission to participate in this study.
	Determine an adequate total of participants	A non-probabilistic, purposive sampling was used. The selected participants shall be selected based on the following criteria: • Get consent from the guardian or representative of guardian. • Age 12-19 years old. • Attended cybersecurity awareness program conducted by Cybersecurity Malaysia. • Willing to respond to the finding of the interview
Planning	Prepare a letter to conduct the observation	Provide a letter to Cybersecurity Malaysia stating the objective and purpose of conducting study through leveraging on cybersecurity awareness program conducted by Cybersecurity Malaysia.
Development	Preparation of observation checklist	Prepare a list of items to be observed during the observation.
	Preparation of the laptops to be installed with Camtasia Studio, Internet browser and Wi-Fi.	Prepare the equipment to be used during the observation.
	What to do during observation	Recording and taking notes.

4.10.1 Instrument Development

The observation of web recording checklist consists of 18 behavioural items. The 18 items developed for this observation checklist (please see Appendix K) include the practices of personal data protection while engaging with online activities such as entering passwords, browsing social media, watching online content, online gaming and etc. The checklist also includes observation of any suspicious activity, characteristics and attitude while browsing the Internet, the message delivered during the cybersecurity awareness program practised by the participants as well as additional information required to be highlighted to participants during the cybersecurity awareness program. The items developed in this observation checklist were derived from the literature

review and findings from the pilot study. Summary for the development of observation protocol is presented in the Table 4.10.

Table 4.10: The Details of Observation of Web Recording Protocol – for Assessment on Behavior

No	Items detail	Reference
1	Does repondent use Internet to watch video?	(Correa et al., 2013; Amanda Lenhart et al., 2010; Madden et al., 2013)
2	Does respondent use Internet to access email?	
3	Does respondent click on any suspicious email?	
4	Does respondent reply or response to any suspicious email?	
5	Does respondent access search engine?	
6	Does respondent use Internet to access online shopping?	
7	Does respondent use Internet to access social media?	
8	Does respondent use Internet downloading song, software, video or film	
9	Does respondent use Internet to play onlien games?	
10	Does respondent click at any pop-up screen displayed?	
11	Does respondent involve in any suspicious communication?	
12	Does respondent click like button at social media?	(Livingstone et al., 2005; Madden et al., 2013)
13	Does respondent give comments at social media?	
14	Does respondent click logout after using Internet application?	(Correa et al., 2013; Amanda Lenhart et al., 2010)
15	Does respondent use password which has more than 8 characters?	(Singh et al., 2007)
16	Does respondent view friend request at social media?	(Livingstone et al., 2005; Madden et al., 2013)
17	Does respondent accept to any friend request at social media?	
18	From your observation, do you see any suspicious activity?	(Livingstone et al., 2005; Ramli et al., 2014; Vandoninck et al., 2014)
19	How do you define youngsters behavior in accessing the Internet?	
20	Does precaution highlighted during cybersecurity awaraness program practiced while youngsters accessing the Internet?	
21	From your observation, what is the additional information required in giving awareness among youngsters particularly in accessing the Internet.	

4.10.2 Data Collection Approach

During observation of web recording, a tool named Camtasia Studio was installed to be used for recording purpose. There were four laptops equipped with Wi-Fi connection. The researcher initially gave a brief introduction on the recording process. Each participant was given 15 minutes duration to be online and was allowed to surf the Internet freely. There were 3 sessions of observation of web recording with 4 participants per session. The Camtasia Studio was used to screen-capture every activity

during the given duration. Audio recordings were also equipped in order to capture any conversation that occurred during the session.

4.10.3 Data Analysis Approach - (Thematic Analysis)

Observation data was analysed manually using thematic analysis. As suggested by Braun & Clarke (2006), thematic analysis is among the common techniques used to analyse qualitative data. It consists of six important steps in order to identify the final themes. Thematic coding is suitable for this study because it can assist the data collected to be translated into meaningful themes. Initially, the recorded observations were checked against the observation checklist. Additional ideas noted during the observation were also added into the observation checklist. The observation checklist was read through many times in order to find initial ideas and codes. Familiarizing with the transcribed data is important in order to acquire initial ideas and understanding. The transcribed data were manually printed, read many times and initial codes noted. The next step was to generate and gather initial codes which in a later step would be organized, revised and its relationships studied to identify redundancies. As the process went along, the finalized codes was transformed into themes and improvised. To ensure the accuracy of steps in thematic analysis, the concept of research trustworthiness as proposed by Lincoln & Guba (1985) was applied and presented in section 4.12. A few iterations of each step were made in order to continually analyse across and between the data until the final theme was formed. Data analysis steps that were taken indicated that sufficient data had been collected to describe the findings.

4.11 DATA COLLECTION PHASE 4 –FOCUS GROUP INTERVIEW

The focus group interview was used as an instrument to measure the result after attending the cybersecurity awareness program. The focus group interview was selected as a strategy of inquiry because it could assist in providing direct information, opinion and feedback from the interviewees. Further, it could promote interviewees to react spontaneously and allow the historical experiences and memories to be revealed (Creswell, 2009). In preparing for the focus group interview, it was required for a set of interview protocol. The interview protocol was a list of suitable questions to be asked during the interview session. The interview protocol for the focus group interview was designed in such a way to gain an in-depth information pertaining to the participants' experiences and viewpoints on a particular topic (Turner, 2010).

Various methods could be used to conduct the focus group interview such as face-to-face interview, telephone, focus group and email. This study applied face-to-face focus group interview. It involved 3 focus groups with 4 persons in each group. This interview was initiated upon receiving consent letters from the participants' guardian (please see Appendix E, F and G). The interview only involved participants from cohort 1 because the saturation point of gaining the required information had been fulfilled. The same participants who were involved in the observation of web recording participated in the focus group interview. The summary of task for focus group interview is presented in Table 4.11.

Table 4.11: Summary of Task for Focus Group Interview

Research Process	Tasks	Activities
Planning	Identify the likely participants to be interviewed	Sent and collect the consent letter from the representative of guardian as a permission to participate in this study.
	Determine an adequate total of participants	A non-probabilistic, purposive sampling was used. The selected respondent shall be selected based on the following criteria: • Get consent from the guardian or representative of guardian. • Age 12-19 years old. • Attended cybersecurity awareness program conducted by Cybersecurity Malaysia. • Willing to respond to the finding of the interview
Development	Prepare a letter to conduct the interview	Provide a letter to Cybersecurity Malaysia stating the objective and purpose of conducting study through leveraging on cybersecurity awareness program conducted by Cybersecurity Malaysia.
	Preparation of recording tools.	Prepare the recording tools for audio and video taped.
	What to do during interview	Recording and taking notes.

4.11.1 Instrument Development

The structured interview was used as an instrument during the focus group interview process. Three sections were developed. Section 1 contained questions pertaining to the participants' background. Section 2 contained questions on problems faced by the participants while being online. Finally, Section 3 contained questions in the form of case examples. The participants were requested to provide ideas and feedback based on the case. The items developed in this interview protocol were derived from the literature review and findings from the initial pilot study. The details of focus group interview protocols are presented in Table 4.12.

Table 4.12: The Details of Focus Group Interview Protocols – for Assessment on Result

No	Items details	References
1	Name	Not applicable
2	Age	
3	Gender	
4	School	
5	Phone number/email	
6	How long you have been used the Internet?	(Correa et al., 2013; Amanda Lenhart et al., 2010; Madden et al., 2013)
7	How many times do you use the Internet?	
8	What are the common applications or website that you frequently visit?	
9	Do you actively using email?	
10	Have you made online purchase?	
11	Have you downloaded song, movie or file from the Internet?	
12	Do you watch movie, video or song in the Internet?	
13	Do you play online games?	
14	Do you know about the threat called identity theft?	(Chawki et al., 2015; Fire et al., 2014)
15	Have you attended any security awareness program before (not this program)?	Not Applicable
16	Can you share any problem that you have faced while engaging in the online activities as you have mentioned before?	(Furnell, 2010; Vandoninck et al., 2014)
17	Have any parties asking for your credentials/ personal data while you are engaging in the online activities?	
18	Have your personal data been used by someone that you have not known?	
19	Do you provide you telephone number while engaging in the online activities?	
20	Do you have any other problem that you would like to share?	

Table 4.12 continued: The Details of Focus Group Interview Protocols – for Assessment on Result

No	Items details	References
21	Scenario 1 (Social Media): You just get back from school. Turn-on your tablet and open your Facebook page. You realized that you can easily browse your Facebook account because you haven't log out from last time you used it. You checked your friend request and got 5 new friends request. Two of the requests are from your classmate but the other three is totally new faces to you. You realized that once acceptance your new friend could access and get your personal data available in your account. Will you approve all five new friends request or only people that you have known personally? Why?	(Lenhart et al., 2011; Livingstone et al., 2005)
22	**Scenario 2 (Email):** It is a weekend time and you have nothing to do except browsing Internet. You turned on your smart mobile and thinking to check your new email from your friend. You have got the email read and realized there was another email from abc@rstu.com. You have never received email from this account before. You opened the email and you were very happy to read that you have selected as one of the winner. For you to claim the prize you need to fill up the form which required your credentials/personal data. Will you fill up the form and reply it back to the senders? Why?	(Amanda Lenhart, 2012)
23	Scenario 3 (Online purchase): Your friend just bought a book from xyz.com. He claimed it was an easy step to follow. You only need to login to the website, select the book, put your details for shipping and finally make payment. The book will be delivered to your doorsteps next three days. In front of your personal computer you have opened the Internet, go the web browsers and type the URL: xyz.com. You can see many books available. You have selected which book you want and ready to go for the next step to enter your credential/personal data for shipping purposes. Click next to make payment but you realized the URL does not start with https://xyz.com. Will you proceed to make payment? Why?	(Kok et al., 2010; Sithira & Nguwi, 2014)
24	**Scenario 4 (Downloading):** You need to install new software that will allow you to convert your file type. Current software that installed in your personal computer is out dated. You tried to browse for the free software available. You have found which suit your need. You have clicked download and the installation begin. During the installation process there is one screen wizard appear and asking for your personal data. It claimed that it will be used for registration purposes. It looks very genuine and trusted. Will you give away your credentials? Why?	
25	**Scenario 5 (Online games):** You frequently play online games with your classmate after school. One day you got invitation from someone outside Malaysia to play games with you. You accepted but suddenly after few games played he request your full name and other credentials/personal data. He claimed that your information will used to book a new released game that you also can't wait to play. He promised he will pay once the game is released. Will you give your information because you really want to play that game?. Why?	

4.11.2 Data Collection Approach

Data collection for the focus interview was collected in cohort 1 only. Initially, the consent letter was given to the representative of the guardians as a permission to collect data from the youngsters. This is a requirement because a youngster is considered as an underage population. Ethically in research underage population requires consent from parents or guardian to participate in a study (Morrow & Richards, 1996). The consent letter was given to representative of the guardian before the program started in order to nominate and return back the form after the program finished. After the program finished, selected participants were grouped into 3 focus groups. An audio and video recording was made on the entire conversation. Approximately 30 minutes of recording was gathered from each focus group. The summary of data collection strategy for phase 3 and 4 is presented in Table 4.13.

Table 4.13: A Summary of Data Collection Strategy for Phase 3 and 4

Cohorts	Date	Place	Phase 3 Participants	Phase 4 Participants
Cohort 1	10th Aug 2015	BTPN (Bahagian Teknologi Pendidikan Negeri Johor), Johor	12	12
Cohort 2	2nd Sept 2015	Sekolah Seri Puteri Cyberjaya, Selangor	None	None

4.11.3 Data Analysis Approach - (Thematic Analysis)

The interview data was analysed manually using thematic analysis. The first step was that all of the interviewed data was manually transcribed from the video and audio tape recording. Familiarising with transcribed data is important in order acquire initial ideas and understanding of pattern. The transcribed data was manually printed and reread many times and initial codes were noted. The next step was to generate and gather

initial codes which were later organised, revised and the relationship was also studied to identify redundancies. As the process went along, the finalised codes were transformed into themes and were then improvised. To ensure the accuracy of steps in the thematic analysis, the concept of research trustworthiness as proposed by Lincoln & Guba (1985) is applied and presented in section 4.12. Few iterations of each step were made in order to continually analyse across and between the data until the final theme was formed.

4.12 RESEARCH TRUSWORTHINESS

In qualitative research, the validity of data can be seen from two perspectives; trustworthiness and credibility. In this study, the validity is performed through adhering to the principle of trustworthiness as suggested by Lincoln and Guba (1985). The principle of trustworthiness in qualitative research is similar to the 'goodness of fit' concept which refers to the degree of accuracy in quantitative research. The concept of research trustworthiness also refers to findings that are 'worth paying attention to' (Lincoln & Guba, 1985). As also proposed by Lincoln and Guba (1985) there are four criteria to be used to determine the principle of trustworthiness in qualitative research as presented in Table 4.14. They are credibility, transferability, dependability and conformability.

Table 4.14: Summary of How the Four Criteria of Trustworthiness were Implemented in this Study

No	Criteria	Description	Tasks
1	Credibility (in preference to internal validity)	Proof that the finding is real and truth.	• Performing literature review and study upon theories and program evaluation model (Chapter 2 & 3) • The real data is obtained from the participated youngsters of cybersecurity awareness program conducted by reliable organization; Cybersecurity Malaysia (Chapter 4) • To ensure the feedback is real recorded and analyze, it has been shared with research participants and supervisors.
2	Transferability (in preference to external validity/generalizability	Proof that the findings is applicable to the other context of research	• Data collection process were presented in details together with its demographic information (Chapter 4) • The number of participant involve in this study is sufficient as indicated by G-Power analysis based on the number of items being asked. • The data reach saturation as all information obtained is interrelated and required no additional information. • Data coded for both quantitative and qualitative data collection technique were based on component of personal data protection and Kirkpatrick Four Learning Evaluation Model. The data coded also based on the formulated research questions. (Chapter 2). • This study involve participants with various demographic profiles, coming from different region across Malaysia and not limited to any geographical boundary (Chapter 3)
3	Dependability (in preference to reliability)	Proof that the findings is consistent and could be repeated in future setting	• The same instrument was used for both Cohort 1 and 2 to ensure consistency in response. • Data were analyzed and findings were reviewed to ensure its accuracy in addressing research questions, conceptual framework, research outcomes and conclusion. • The pupose of qualitative study is to verify the data collected through quantitative study. Even though only cohort 1 is involved, the distribution of participant demographic background is varies as this participants came from all over Malaysia. This is because the cybersecurity awareness program is conducted at national level which involve participants from different state in Malaysia.
4	Conformability (in preference to objectivity)	Proof that the study is set at neutral setting. The findings are drawn from the real data which do not involve researcher personal idea, interest, motivation and biasness.	• The real data is obtain from the participated youngsters of cybersecurity awareness program conducted by reliable organization; Cybersecurity Malaysia (Chapter 3) • The entire data collected were recorded. • Finding from this study were shared with the expert from Cybersecurity Malaysia for validation and confirmation purposes.

4.13 VALIDITY AND RELIABILITY OF INSTRUMENTS

The concept of validity and reliability is important in conducting quantitative research to ensure the accuracy of the instrument used throughout the study. This study constructed and developed its instrument based on findings in the literature review and theoretical foundation, thus require careful examination to ensure the instruments being used in this study is valid and reliable to address the research objective. The instruments that require confirmation on its validity and reliability are the survey for assessment on reaction and the pre-test and post-test survey for assessment on learning. These instruments underwent content validity and field testing to ensure its reliability. The detail of the validity and reliability establishment is discussed in the following sections.

4.13.1 Validity

Validity, according to Wainer and Braun (2013), is 'appropriateness,' 'meaningfulness' and 'usefulness' measurement of research instrument for a study. It serves the purpose of ensuring the constructed instrument truly measures what the study intended to measure. The first stage in ensuring the validity for this study was that the instruments were thoroughly checked for any difficulty in understanding certain words, clarity and logical flow of questions to minimise logical error. The next step was that this study used content–related evidence of validity as proposed by Haynes, Richard, & Kubany (1995). The content–related evidence of validity is a set of collective evidence via expert judgment reviews. Two appointed panel of experts from University of Malaya and International Islamic University of Malaysia were chosen based on their expertise and familiarity with the research context (please see Appendix B and C).The appointment of the two experts also help to minimize bias in instrument development.

The appointed panel were given the hardcopy and softcopy of each set of instruments. They were provided with two week duration to review and offer comments. Principally, the instruments were thoroughly checked against its suitability, significance of content and focus of the instrument. After gaining comments from the panel of experts, possible amendments were discussed among peers before making modifications and revision to the instruments.

4.13.2 Reliability

The measurement of reliability is another important aspect to ensure a degree of consistency for the instruments (Carmines & Zeller, 1979). This study tests the reliability through a field test procedure. The field test is meant to test for items that are deemed unsuitable to be included in the survey. The field test is set on a real setting of data collection by leveraging on an actual cybersecurity awareness program conducted by Cybersecurity Malaysia. A total of 50 youngsters from a total of 300 participants were given the survey as in an actual data collection procedure. The instruments were collected after they finished answering it. The duration of time required was also recorded. Apart from their written answer, any verbal comments and suggestion were also noted. Based on their answer and comments, changes were made to the instrument accordingly after it underwent peer review for verification. Several modifications were made to the instruments including removing confusing questions. The modified version of the instruments was again checked to ensure that all items being asked are applicable to the research questions.

4.14 CHAPTER SUMMARY

This chapter discussed the research methodology and strategies used in this study. It also briefly defined the research process, the selection of population and sample as well as construction of instruments. Each phase of data collection technique was briefly discussed. This chapter also highlighted the aspect of research trustworthiness and discussed what strategies were used to establish the validity and reliability for this study. In the next chapter, analysis and findings from the data collection is discussed and explained, which leads to the proposed solutions.

CHAPTER 5

DATA ANALYSIS AND FINDINGS

5.1 INTRODUCTION

This chapter describes the method of analysis in detail, and its findings. The details consist of how the analysis carried out for each of data collection phase (data collection Phase 1: survey, Phase 2: pre-test and post-test survey, Phase 3: observation of web recording and Phase 4: focus group interview. Each data collection phase applied different types of data analysis techniques. The findings for each analysis are presented accordingly.

As described in Chapter 4, Phase 1 of the data collection for assessment of reaction (survey) was analysed using Multiple Regression, Phase 2 of the data collection for assessment on learning (pre-test and post-test survey) was analysed using Wilcoxon Signed Rank Test and Phase 3 and Phase 4 assessments on behaviour (observation of web recording) and result (focus group interview) were analysed using thematic analysis. The findings from Phase 1 and Phase 2 were merged and combined with findings from Phase 3 and Phase 4 in order to answer the research questions posed earlier in this thesis.

In this chapter, the findings are presented in four sections according to data collection phases in the previous chapter. Section 5.3 describes the finding for Phase 1, section 5.5 describes the finding for Phase 2, section 5.7 describes the finding for Phase 3 and section 5.9 describes the finding for Phase 4. The final section of this chapter presents

how findings were merged and used to answer the formulated research questions. The answers to the formulated research questions are presented in the next chapter.

5.2 DATA ANALYSIS FOR PHASE 1

For the data analysis in Phase 1, 384 surveys obtained after deleting missing values were used and keyed-in into SPSS. Items for Section 1 were analysed using descriptive analysis meanwhile item for section 2, 3 & 4 were analysed using Multiple Regression technique. The descriptive analysis is meant to determine frequency of demographic profile from this study with no assumptions required. For multiple regression analysis there are four main assumptions which are required to be fulfilled. According to (Ho, 2014; Stolzenberg, 2004) the four main assumption for multiple regression analysis presented in the following Table 5.1

Table 5.1: Assumptions of Multiple Regression Analysis

Assumption	Description
Linearity	The relationship between dependent and independent variables must be a linear relationship and it can be explain by residual plots.
Homoscedasticity	The assumptions of equal variances between pair of variables. This is also can be explain by residual plots
Independence of error terms	The predicted value is independence and not related to any other prediction. This could be explaining by observing the Durbin-Watson *d* statistics. If *d* statistics is between the two critical values of 1.5< d <2.5, it shows no linear auto-correlation in the data.
Normality	The difference between the obtained and predicted dependent variable scores. Also explained by residual plot.

The detail for descriptive analysis and Multiple Regressions is presented in the following section.

5.3 FINDING FOR PHASE 1

The finding starts with the descriptive analysis of the demographic profile of the sample. The finding is for Section 1 (Question 1-7) (please see Appendix I). The demographic profile consists of gender, age, access to the Internet, usage of the Internet, duration of Internet usage, previous attendance to any cybersecurity awareness program and awareness on identity theft. The summary of the descriptive analysis in terms of frequency for each question asked for demographic profile is as Table 5.2 below:

Table 5.2: Summary of Descriptive Analysis in Term of Frequency for Each Question Asked for Demographic Profile

Demographic Profile (n=384)		**Responses (N)**	**Percentage %**
Gender	Male	36	90.6
	Female	348	9.4
Age	12 years old	0	0
	13 years old	51	13.3
	14 years old	99	25.8
	15 years old	134	34.9
	16 years old	38	9.9
	17 years old	60	15.6
	18 years old	1	0.3
	19 years old	1	0.3
Access to the Internet	Yes	379	98.7
	No	5	1.3
Internet usage	Social Media	Yes - 351 No - 33	Yes - 91.4 No - 8.6
	Sending and reading email	Yes - 359 No - 25	Yes -93.5 No - 6.5
	Watching online video	Yes - 351 No - 33	Yes - 91.4 No - 8.6

From Table 5.2, based on the descriptive analysis made on the demographic profile, majority of the participants were female; this is because cohort 2 involved a cybersecurity awareness program conducted at an all-female school. The sample consists of 12-19 year olds in which this study managed to get participants from all ages in the stated range, except for 12 years old. For the Internet usage, majority of the participants were involved in the usage of social media, sending and reading email,

watching online videos and downloading. Meanwhile, fewer participants used Internet for playing games and online shopping. Almost half of the youngsters used the Internet daily while others used the Internet only during weekends. From the descriptive finding, the percentage of those who have attended, and those who have never attended any cybersecurity awareness program is approximately equivalent. Majority of participants realised the risk of identity theft of their personal data.

Section 2 in phase 1 of the data collected, the items asked were pertaining to the feedback from youngsters regarding the program content. Summary of findings for Section 2 of the data collection is presented as the following Table 5.3.

Table 5.3: Summary of Findings for Section 2 Data Collection Phase 1

Items ID	Items asked	Mean
PC1	I understand the program objective is to educate youngsters about safety in cyber world	4.53
PC2	I found this program is joyful and attractive.	4.15
PC3	I found the material used is useful to enhance the practice of personal data protection.	4.38
PC4	I found the program content is relevance for me to enhance the practice of personal data protection.	4.42
PC5	I felt this program has been presented at the right level to enhance the practice of personal data protection.	4.30
PC6	I understood the importance of protecting personal data.	4.38

Based on Table 5.3, there were six items asked in Section 2. Each of the items was given an ID for easy reference. Each item was analysed based on the mean score of 3 (neutral). From the result, each item asked has a mean score above 3. Therefore it can be said that the content presented during cybersecurity awareness program on personal data protection were understood by the participants.

In section 3 of phase 1, the items asked were pertaining to the program features. The summary of findings in Section 3 of the data collection is depicted as per Table 5.4 below.

Table 5.4: Summary of Finding for Section 3 Data Collection Phase 1

Items ID	Items asked	Mean
PPC1	The presenter has good knowledge about personal data protection.	4.46
PPC2	The presenter has explained clearly about personal data protection.	4.44
PPC3	The presenter has given example about personal data protection.	4.46
PPC4	The presenter has encouraged the participants to have better understanding about personal data protection.	4.48
PPC5	I found the activities during the session help me to have better understanding about personal data protection.	4.38
PPC6	I found the session about personal data protection is too long.	3.71
PPC7	I found that session about personal data protection require additional content.	3.73
PPC8	I found the session about personal data protection is useful.	4.35

Based on Table 5.4, there were 8 items asked and comparisons were made based on the mean score values. The mean score values of all the items were above 3 (neutral). Overall, the participants found that the presenter had good capability in giving awareness on personal data protection. However, the participants found that the session was too long and required additional content. In section 4 of phase 1 of the data collected, the items asked were pertaining to the benefit gained from the cybersecurity awareness program. The summary of findings for Section 4 is depicted as the following Table 5.5.

Table 5.5: Summary of Finding for Section 4 Data Collection Phase 1

Items ID	Items asked	Mean
PB1	My knowledge about personal data protection has increased.	4.42
PB2	I'll practice the knowledge gained through this session to protect my personal data protection.	4.39
PB3	Now, I know how to protect my personal data.	4.41
PB4	Now, I know how to contact the responsible party if any third party ask or steal my personal data.	4.39
PB5	Now, I know how to act if any third party ask or steal my personal data.	4.36
PB6	Now, I know the importance to protect personal data protection.	4.43

From Table 5.5, which is also based from the mean value score, all items asked recorded of score above 3 (neutral). Overall, the participants found that the session gave them benefits, and their knowledge on personal data protection had increased. The calculation of mean for program content, program features and program benefit were compute accordingly using SPSS in order to conduct multiple regression analysis. Basically the determinant of positive reaction among youngsters is based on the relationship between program content and features (independent variables) and program benefit (dependent variable.

After computing the mean score for program content, program features and program benefit, the first step is to determine the assumption of linearity, homoscedasticity, normality and independence of error terms through regression analysis. Based on the analysis result the following assumption is answered as presented in Table 5.6. The details of analysis are depicted in Appendix R.

Table 5.6: Summary of Analysis for Assumptions of Multiple Regressions

Assumption	Description	Findings
Linearity	The relationship between dependent and independent variables must be a linear relationship and it can be explain by residual plots.	The scatterplots of standardized residuals against the standardized predicted value shows no clear relationship pattern. This is consistent with the assumptions of linearity and homoscedasticity.
Homoscedasticity	The assumptions of equal variances between pair of variables. This is also can be explain by residual plots	
Independence of error terms	The predicted value is independence and not related to any other prediction. This could be explaining by observing the Durbin-Watson *d* statistics. If *d* statistics is between the two critical values of $1.5< d < 2.5$, it shows no linear auto-correlation in the data.	As the Durbin-Watson d=1.774 is between the two critical values of $1.5< d < 2.5$, it can be assumed that there is independence of residuals.
Normality	The difference between the obtained and predicted dependent variable scores. It can be explain by residual plot also.	Base on the P-P plot of standardized residuals, it can be seen that the plot of the residuals for the dependent variable fits the expected pattern which indicate normal distribution.

Thus it can be concluded that all assumptions are fulfilled. The next step is to evaluate the prediction equation, evaluating the strength of prediction equation, identifying multicollinearity and independent relationship. For the prediction equation, the following formula is used $Y' = A+B_1X_1 + B_2X_2 + \ldots.B_nX_n$ where Y' = the predicted dependent variable, A = constant, B = Unstandardized regression coefficient and X = value of predictor value. The value for each component in this formula is derived based on the coefficients table of multiple regression analysis. In order to predict the program benefit positive reaction attributed from program content and program features, the value presented in the Unstandardized Coefficients column. Therefore the predicted equation would be:

Predicted program benefit positive reaction attribution = 0.67 + (0.45*5) + (0.41*5), resulted in 4.97. The value of 5 is used the maximum positive reaction based on the Likert scale 1 until 5. Given that program benefit positive reaction attribution is measured on 5 point scale with 1 = strongly disagree, to 5 = strongly agree, a predicted

value of 4.97 would suggest that program content and program features would attribute to program benefit in the form of positive reaction among youngsters.

The next step is to evaluate the strength of prediction equation in the form of *R*-square (coefficient of determination). An indicator of *R*-square = 0 is used to indicate no linear relationship between the predictor and dependent variables, analysis of variance (ANOVA) is utilized in this step. In ANOVA test, the *F* value is served to test how well the regression model fits the data. *F* value is computed at 278.90, with observed significance level of less than 0.0001. Hence, no linear relationship between the predictor and dependent variables, which means linear relationship, is established.

Further analysis into the data is to identify multicollinearity, this is because when predictor's variables correlated among themselves it is difficult to assess the attribution of each predictors. The way to determine the degree of multicollinearity is by observing the value of VIF value in coefficient table. The condition suggested the VIF value must (less than 10) for it to be acceptable. Based on the analysis, the VIF value is computed at 2.20. Thus multicollinearity does not appear to be a problem in this case.

The final step is to determine the independent relationship by observing the Beta weight (β) in coefficient table. From the coefficient table, it can be determined that program content (β) = 0.45, t=9.302, p<.0001 has the strongest relationship with program benefit positive reaction attribution. Based on the analysis steps, the youngsters feels the program content and program features is benefited to them and this also provide evidence of positive reaction among participants.

5.4 DATA ANALYSIS FOR PHASE 2

For data collection Phase 2, the same unit of analysis was used as in section 4.5. For the analysis, SPSS was used to initially determine the type of data collected, whether or not it was normally distributed. The main purpose of analysis on the data collected for assessment on learning is to measure the difference of awareness of the youngsters before and after attending the cybersecurity program. The feedback from both the pre-test and post-test surveys that were distributed to the participants were manually keyed-in into SPSS and saved as a .sav file. The first step of data analysis was to determine the type of data collected. From table 5.7, the next step is to group the data into categories and cumulative scores were calculated. The initial collected data (Pre-test) and initial collected data (post-test) refers to the list of items asked in the survey. Since this survey applied Likert scale as a way to gain feedback from participants, each answer was assigned to a number. For instance, 1 referred to strongly disagree while 5 is referred to strongly agree. These scores were calculated as cumulative scores. The cumulative scores were used to compare the result of the pre-test and post-test.

Table 5.7: Grouping for Cumulative Score (Pre-test and Post-test)

Initial collected data (Pre-test)	Grouping (Pre-test)	Initial collected data (Post-test)	Grouping (Post-test)
Pre_Knowledge_1 Pre_Knowledge_2 Pre_Knowledge_3 Pre_Knowledge_4 Pre_Knowledge_5 Pre_Knowledge_6 Pre_Knowledge_7 Pre_Knowledge_8 Pre_Knowledge_9 Pre_Knowledge_10	Pre-test_Knowledge	Post_Knowledge_1 Post_Knowledge_2 Post_Knowledge_3 Post_Knowledge_4 Post_Knowledge_5 Post_Knowledge_6 Post_Knowledge_7 Post_Knowledge_8 Post_Knowledge_9 Post_Knowledge_10	Post-test_Knowledge
Pre_Skill_1 Pre_Skill_2 Pre_Skill_3 Pre_Skill_4 Pre_Skill_5 Pre_Skill_6 Pre_Skill_7 Pre_Skill_8	Pre-test_Skills	Post_Skill_1 Post_Skill_2 Post_Skill_3 Post_Skill_4 Post_Skill_5 Post_Skill_6 Post_Skill_7 Post_Skill_8	Post-test_Skills
Pre_Attitude_1 Pre_Attitude_2 Pre_Attitude_3 Pre_Attitude_4 Pre_Attitude_5 Pre_Attitude_6 Pre_Attitude_7 Pre_Attitude_8 Pre_Attitude_9	Pre-test_Attitude	Post_Attitude_1 Post_Attitude_2 Post_Attitude_3 Post_Attitude_4 Post_Attitude_5 Post_Attitude_6 Post_Attitude_7 Post_Attitude_8 Post_Attitude_9	Post-test_Attitude

Based on the normality test to determine whether the collected data were normally distributed or not, it was revealed that the data were not normally distributed. Therefore the normal *t*-test cannot be used to compare the score. As suggested by Ho (2014), in the case of violation of normality, the Wilcoxon test is an appropriate alternative test to compare the score between the pre-test and post-test.

5.5 FINDING FOR PHASE 2

The finding for data collection Phase 2 for the pre-test and post-test survey was started by analysing the type of data collected. This is important to identify whether the data collected is normally distributed or non-normally distributed. In SPSS, the normally distributed data is commonly known as parametric data and non-normally distributed data is commonly known as non-parametric data. According to Ho (2014), the normality

of data is based on the skewness and kurtosis values which indicated by the *z* value. If the calculated *z* value exceeds the lower limit of -1.96and upper limit over +1.96, the normality of data is rejected. In this study, the *z* value was calculated as, skewness: 1.877/0.123 = 15.26 and kurtosis = 1.530/0.246 = 6.22 which exceeded +1.96, thus the data is considered not normally distributed.

The first step in determining the type of data collected is important because it would identify a suitable statistical test to be used in comparing the pre-test and post-test result. Also, according to Ho (2014), if a violation of the normality data occurs, the suitable type of statistical test to be used for comparison between pre-test and post-test score would be the Wilcoxon test. The Wilcoxon test is suitable to analyse a set of data collected from the same individuals as in this study. Cumulative scores derived from the pre-test and post-test scores were compared using the Wilcoxon test. The result from the Wilcoxon test was tested against the following assumptions: These assumptions were developed based on the conceptual framework for Level 2 assessment to measure changes in knowledge, skills and attitude.

i) The knowledge of participants does not change after attending the cybersecurity awareness program.
ii) The skill of participants does not change after attending the cybersecurity awareness program.
iii) The attitude of participants does not change after attending the cybersecurity awareness program.

Table 5.8: Wilcoxon Signed Rank Test for Data Collection 2 (Pre-test and Post-test)

Wilcoxon Signed Rank Test			
	The total score of post-test knowledge - The total score of pre-test knowledge	**The total score of post-test skills - The total score of pre-test skills**	**The total score of post-test attitude - The total score of pre-test attitude**
Z	-3.105[b]	-3.678[b]	-1.324[b]
Asymp. Sig. (2-tailed)	.002	.000	.186

Based on the Wilcoxon test, the statistical result is shown in Table 5.8, the p>0.05 was used to determine the level of significance. The critical value of *z* must be within -1.96 and +1.96. In SPSS, the Wilcoxon statistic is converted into a *z*-value which can be tested for significance under the normal curve of data distribution (Ho, 2014). Since the obtained *z* value were *z* (-3.105) for measuring knowledge, and *z* (-3.678) for measuring skills, assumptions (i) and (ii) are rejected. Thus this shown that after attending cybersecurity awareness program, knowledge and skills of participants changed. Meanwhile for attitude, the result is different which gave insignificant result where *z* (-1.324) was found to support the assumption number (iii). Thus, the attitude of participants did not change after attending the cybersecurity awareness program. This result could be disputed as only knowledge and skills were reported to change as compared to attitude. Attitude requires longer time to change and under certain circumstances. Thus, a continuous effort in making cybersecurity awareness is deemed essential in order to change the participants' attitude.

5.6 DATA ANALYSIS FOR PHASE 3

In Phase 3, the data analysis technique used for observation of web recording was thematic analysis (Braun & Clarke, 2006). The thematic analysis is suitable for this study because it consists of rigorous steps in finding initial codes, themes and possible

components of analysis inclusive of ideas and requirements to conduct additional observation. The steps are i) becoming familiar with the data ii) generating initial codes iii) searching for themes iv) reviewing themes v) defining and naming themes vi) producing a report.

The observation of web recording was done based on the earlier prepared observation checklist (refer to Chapter 4 subsection 4.10.1). A total of 12 separate observation checklists were recorded from 3 focus groups. These checklists were combined with the additional field note written during the observation session. In order to generate initial ideas and codes through the observation checklist, the checklist had undergone many reread process, carefully examined and analysed to obtain a better sense of the observation. In the early stage of implementing thematic analysis, the initial codes were derived based on the following aspect: components of suspicious behaviour among participants, attitude in browsing the Internet, behaviour practiced after attending the cybersecurity awareness program and additional elements found necessary to make participants aware on the importance of protecting personal data. Initial codes gathered based on the above components were revised, examined and thoroughly checked for relationships and any redundancies that might occur before producing themes. A theme refers to important patterns found in the data that could provide answers to the research questions. The final effort in data analysis for observation of web recording was to generate main themes by categorising and refining specific name given to each theme together with its clear definitions and supporting literature.

5.7 FINDINGS FOR PHASE 3

The findings for data collection Phase 3 were derived from six important steps in the thematic analysis. This section briefly discusses each step taken before the final finding

from the observation was derived from the web recording. The steps in thematic analysis involved:

i) Becoming familiar with the data

In this step, the process of transcribing and combining the collected data through the observation checklist and notes taken during the observation session was done. Then, the data was read by a researcher many times in order to understand the flow and pattern, and the initial idea was then noted. It was necessary to read the data repeatedly before starting with the coding process in order to identify the pattern of collected data. To ensure the pattern accuracy, the collected data was checked against the observation checklist.

ii) Generating initial codes

To generate initial ideas, notes were written manually beside the collected data and retyped in Microsoft Word for easy reference. The code was meant to identify the feature of the data and to organise them into categories. Each category of codes is given its own definition. It is important to work systematically on the collected data by giving equal attention to each data. The initial codes were gained based on the following aspect of observation which were components of suspicious behaviour among participants, attitude in browsing the Internet, behaviour practiced after attending the cybersecurity awareness program and additional elements required to make the participants aware on the importance of protecting personal data. The sample of initial codes gathered is presented as the following Figure 5.1. This table consists of three columns, data extract is for the actual data collected, coded for is for the initial coding and definition column is meant to provide clear definition of the codes. [Y0] indicates the identification number assigned to participant.

Data Extract (Skills)	Coded for	Definition
Not clear cache not shut the screen. [Y1]	Gets thing done in rush	Youngsters tend to be forgetful and lack of focus during engaging in online activities.
Respondent immediately "click" at the email "to confirm email address. The early evaluation is required before clicking the email. [Y10]	Think before act	Individual judgement is important role in protecting personal data.
Do not close the screen. [Y10]	Gets thing done in rush	Youngsters tend to be forgetful and lack of focus during engaging in online activities.
Open gay song. [Y6]	Enthusiast feeling to discover	The discovery will among youngsters is high. They are free to browse sometimes without restriction.
He just watched YouTube by opening two songs. The song source looks genuine.[Y4]	No restriction in Internet browsing	They are free to browse sometimes without restriction.
No clear cookies. Not logout twitter just click close. Same password used within various applications. [Y9]	Gets thing done in rush The risk of password	Youngsters tend to be forgetful and lack of focus during engaging in online activities. The awareness about using password in online activities is lack.
Data Extract (Attitude)	**Coded for**	**Definition**
Too fast. Sometimes less thought were given. He used different password for different application. Less risk if someone wants to hack his personal account. [Y10]	Think before act The risk of password	Individual judgement is important role in protecting personal information. Certain youngster has awareness upon how to manage password in online activities.
Practiced security culture by having the following. Logout after used his email. Removed his email account from the stored email list inside the computer. He seems understand the concept of security while using an Internet. [Y2]	Clean cookies after browsing the Internet	Has awareness on how to clear trace after using the computer.

Figure 5.1: Sample of Generated Initial Codes at the Early Stage of Data Analysis

iii) Searching for themes

The third process involved looking at the initial codes from a bigger picture, which is also known as a theme. In order to identify the themes, line-by-line analysis of the collected data were done manually and the different codes were sorted into potential themes. The process of collating and combining different codes also occurred here

which eliminates any redundancies which were found to be unrelated to the study. The line-by-line analysis was important because it allows for rich and complex narratives. The process of determining the themes was done manually. When the line-by-line analyses had been done, the notes on the texts were analysed by using highlighter pens to identify potential patterns. This is because; this kind of technique is suited for rich and complex narratives. A technique to discover themes in qualitative data is important in order to describe, compare, and explain regarding the data pattern. The themes identified in this step were gathered and illustrated using the thematic map. The purpose of having a thematic map is to show the relationship of each theme and sub-themes. The thematic map was developed based on the list of initial codes categorised into three main themes which were behaviour outcome, undesirable behaviour and desirable behaviour together with their sub-themes. A sample of initially identified themes using the thematic map is presented as the following Figure 5.2.

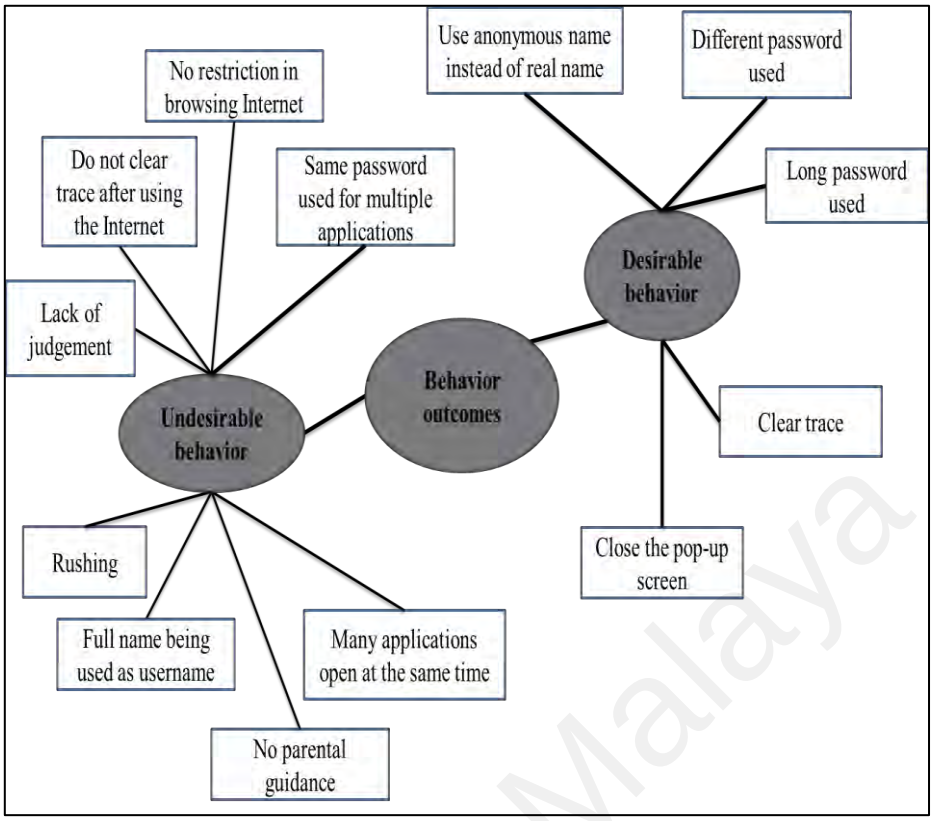

Figure 5.2: Sample of Initial Identified Themes Using Thematic Map

The list of initial codes based on behaviour outcomes were further categorised into undesirable behaviour and desirable behaviour. The undesirable behaviours that were found were; same password used for multiple applications, no restriction in browsing the Internet, do not clear trace after using the Internet, lack of judgement, rushing, full name being used as username, no parental guide and using many applications at the same time. The desirable behaviours that were found were; close the pop-up screen, clear trace after using the Internet, long password used, different password used for different applications and use anonymous name as username. These themes were further reviewed and refined many times in order to select the best themes to answer the developed research question.

iv) Reviewing themes

Step 4 involves reviewing the themes gathered as above. During this step, the initial themes were checked against its relationship to personal data protection. This was to

ensure that only themes and sub-themes which were related to personal data protection are remained. Based on Figure 5.3, the two finalised themes were undesirable behaviour and desirable behaviour. The theme of behaviour outcome was disregarded because it was considered too general to be considered as a theme. There were also sub-themes that were removed because they were found to be irrelevant to personal data protection. Each finalised theme had its own sub-themes. For undesirable behaviour, the sub themes were; same password used for multiple applications, no restriction in browsing the Internet, do not clear trace after using the Internet and lack of judgement. For desirable behaviour, the sub-themes were clear trace after using the Internet, different and long password used, use anonymous name for username and close the pop-up screen.

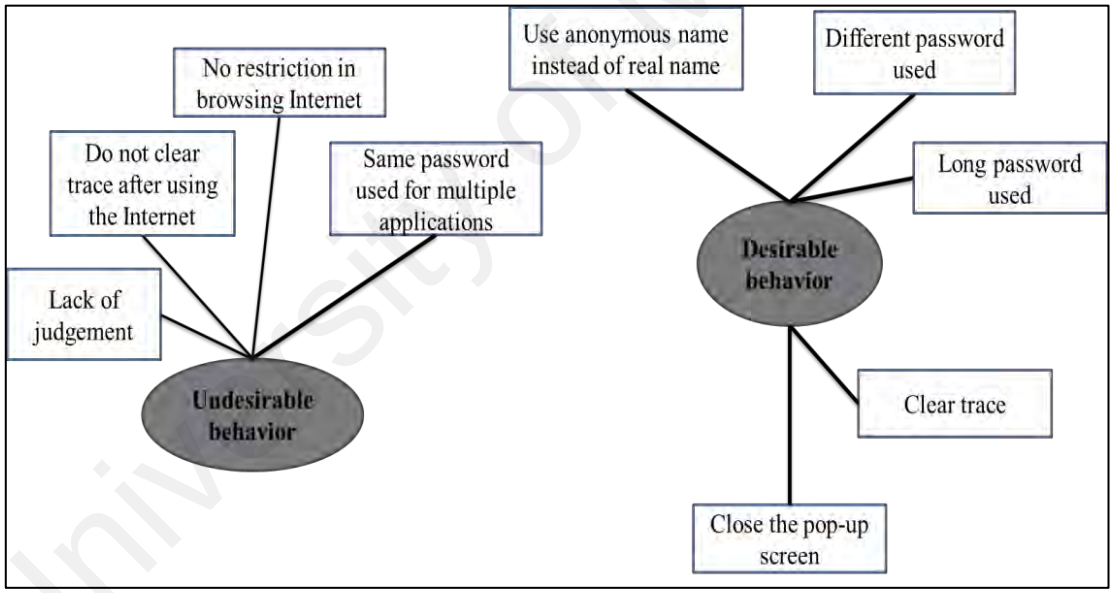

Figure 5.3: Sample of Reviewed Theme

v) Defining and naming themes

In this step, each theme and its sub-themes were gathered in one table as per Figure 5.4. This table also includes real observation data as well as supporting literature to ensure the identified themes were valid to be considered as a theme. The process of reviewing

the themes involved cross-checking those with data extracted during the observation of web recording. This was to ensure consistency and provide evidence to support each theme. The sample of identified themes together with its sub-themes and real observation is presented as per Figure 5.4

Themes	Sub-themes	Real observation	Related Literature Review
Undesirable behavior **Definition:** Not favorable actions	Do not clear trace after using the Internet **Definition:** The browsing history remain	Not clear cache, not shut the screen **[Y12]**	*"An advertiser can track a user's movements between Web sites because the first banner advertisement presented can set a cookie containing a unique identifier. As subsequent advertisements are read, the advertiser can construct a profile about a user based on the cookies it receives from the user"* (Sit & Fu, 2001)
	Lack of judgement **Definition:** Capability of making decision	Respondent immediately "click" at the email "to confirm email address. The early evaluation is required before clicking the email **[Y10]**	*"Substantial proportion of young Internet users may lack the good judgment"* (Beebe, Asche, Harrison & Quinlan, 2004)
	No restriction in browsing the Internet **Definition:** Free browsing of the Internet	Open gay song. **[Y6]**	*"Those aged 15 and 16 reported to surf the Internet without any restrictions being placed"* (Álvarez, Torres, Rodríguez, Padilla & Rodrigo, 2013)
	Same password used for multiple applications **Definition:** One password used for all	Same password used within various applications. **[Y9]**	*"They also used the same password and username to other social networking website accounts"* (Haron & Yusof, 2010)

Figure 5.4: Sample of Themes and its Definition and Supporting Literature

vi) Producing a report.

The final step was to produce a report of complete analysis based on the data collected from the observation of web recording. Thus, this section briefly reports on the processes involved.

5.8 DATA ANALYSIS FOR PHASE 4

In order to analyse the interview data, the same deductive approach, by applying thematic analysis (Braun & Clark, 2006). This method of analysis was used due to its flexibility and ability to produce accessible reports to the public, and particularly applicable to this study, which is to fulfil the formulated research objectives. Basically, the same steps were implemented for the data analysis collected through the focus group interview sessions. In brief, once the interview session was completed, the data was transcribed and been read many times in order to identify patterns and themes across it. Variety of themes, initial codes and researcher's ideas were recorded in hardcopies and softcopies.

A total of 4 audio recordings were obtained with duration of approximately 1 hour and 8 minutes were transcribed. The transcripts were thoroughly checked and properly examined in order to gain a complete understanding of the interview. The interview questions were developed on the basis of measuring the result or impact of cybersecurity awareness program. The interview questions include queries on the understanding level among participants regarding personal data protection, problems faced in engaging online activities as well as their feedbacks, thoughts and actions based on the sample cases given during the interview session. In order to generate themes from the interview scripts, the following components were used: desirable behaviour, security culture practices, management of behaviour by participants and necessary assessment component.

5.9 FINDINGS FOR PHASE 4

Findings for the data collection in Phase 4 were derived from five important steps of the thematic analysis. This section briefly discusses each step taken before the final finding derived from the interview. The steps in the thematic analysis involved:

i) Becoming familiar with the data

In this step, the process of transcribing data for each focus group interview was based on recorded audio and video. The transcribed data was repeatedly read in order to understand the flow and pattern, as well as to find initial ideas which later formed the themes. It was necessary to read the data repeatedly before findings from the initial coding can be started. At this stage, it was also important to identify patterns in the collected data. To ensure the accuracy of the patterns, the collected data was checked against the audio and video recording of the interview. The transcribed data was systematically arranged based on the same questioned asked to each focus group. These were important steps before starting to generate the initial ideas. Figure 5.5 presents the interview transcriptions arranged according to the focus groups with [Y0] indicates the identification number assigned to a participant.

115 Researcher: Do you know about the threat called identity theft or you just have heard it from the
116 session just now.
117 [Y5]: Definitely. Especially in the reality TV made in the America. Catfish TV. I'm not sure
118 about it talk about the threat identity theft they took the trick become someone else and do frank
119 to other people.
120 Researcher: Ok. How about [Y6]?
121 [Y6]: What is identity theft?
122 Researcher: is actually someone steal you identity and use it for any illegal used, so you have
123 make sure that your identity is not being available too much over the Internet. How about [Y7]?
124 [Y7]: Yes I know identity theft.
125 Researcher: and [Y8]?
126 [Y8]: I knew this because when I was started using Facebook but I plan to take it seriously when
127 I join this discourse about the danger of it.
128 Researcher: Ok. The last question for this section is having you ever attended any cyber security
129 awareness session instead of this one. So [Y5]
130 [Y5]: Oh no. This is the first one. Initially
131 Researcher: Ok next question is about problem that you've faced before you attending this cyber
132 security awareness session. Can you share with me any problem that you have faced when you
133 browsing the Internet. Start with [Y5]. Anything's that border you

Focus group 1	Focus group 2'	Focus group 3
Question 2: So how many times do you use Internet in a day? Ryan: No limitation because they think I big and able to differentiate. [Y2]: It depends actually if I'm free it like use all day and if I have homework or other stuffs there will be like 2-3 hours [Y3]: 3 hours, 4 hours [Y4]: Yes, it all depends like 1 to 3	Question 2: So how many times do you use Internet in a day? [Y5]: Erm depend on the situation, if I were giving project to do based on using the Internet and then I have to used it but then but in normal days I don't because in normal days because I don't have any social media. [Y6]: There wasn't a single day that I didn't use the Internet. [Y7]: If there is Internet connection I'll be using. [Y8]: Arr. Internet usage depend on the situation let for example if I had a competition and I need a lot of points normally it could even take one whole day. 24hrs but let say I've nothing to do I just go and check my social media to find what post they have.	Question 2: So how many times do you use Internet in a day? [Y9]: : If it is weekend maybe around 10 it depends I play games online so ya if during weekdays around 3-5 [Y10]: I periodically used the Internet rr I'm not erm I don't really use it every day but once I have a need to used it like let say I have a tough question that I couldn't answer in my homework I'll used the internet. Sometimes in a day I don't use it sometime in a day I use it. [Y12]: The same with [Y11] and [Y9] [Y11]: I also play games but during weekdays since we have school we basically at the school like since 6 till 6 so.

Figure 5.5: Sample of Interview Transcription

ii) Generating initial codes

In order to generate the initial codes, the arranged interview transcription was manually printed and initial ideas were noted down and later transferred into Microsoft Word to be used for the next step. Equal attention was given to each collected data. The initial codes were gained based on the following aspect of information required which were desired behaviour on protecting personal data among participants, security culture on protecting personal data, management of behaviour in the digital world and assessment component required. The sample of initial codes gathered is presented as in Figure 5.6. This table consists of three columns, "data extract" is for the actual data collected, "coded for" is for the initial coding and "definition" column is meant to provide clear definition of the initial code.

Data Extract	Coded for	Definition
Question 11: can you share any problem that you face while engaging to the online activities. [Y1]: Problems. I think the most obvious one is slow internet connection. Security aspect, well occasionally there will be some spam, stuff coming in like ads like you are getting 100000 so I don't really buy it. [Y2]: Sometimes when they are using your laptop or your computer it will come the advertisement that sometimes might border you right so with inappropriate stuff so [Y3]: advertisement scam [Y6]: The Internet connection. And sometimes the videos in you tube not available in your country. [Y7]: Ad and crash. The software crash. [Y8]: It is always the advertisement and the so every time I need to get a particular things that I need installing software or patch, it happen when the entire website is not secured and safe.	Self-realization about the harmful effect. Think before act. Trust Self-realization about the harmful effect Realized but wanted to try Love to trial Know how to differentiate the legitimate and illegitimate Problem: Slow internet connection Ads (mostly about ads) YouTube not available in Malaysia Software crash Waste of time Chat room/massager	List of identified problem faced by participants.

Figure 5.6: Sample of Initial Codes from each Interview Question

iii) Searching for themes

The third process involved looking at the initial codes from a bigger perspective, which is known as themes. In order to identify the themes, the same steps depicted in section 5.7 were used. There were 4 main themes and 43 sub-themes developed initially. The main theme was desired behaviour, security culture, management of behaviour and

assessment component. Unlike applying the same step in data analysis of Phase 3, the presentation of themes and its sub-themes in this analysis was in a form of a table due to a number of sub-themes which could not be presented in the form of a thematic map.

Main themes	Desired behavior	Security Culture	Management of behavior	Assessment component
1	Think before act	Extra precaution	Managing peer influence	Level of IT Literacy
2	Determine the level of trust	Self-realization about the harmful effect	Managing time in accessing the Internet	Personality background
3	Think about privacy	Differentiate between legitimate and illegitimate	Managing social interaction in online environment	Perception of individual
4	Not trusting outsider or stranger	Double checking strategies	Level of sharing information	Parenting guidance and level of control
5	Trust common sense	Reliability concept	Managing discovery will to try on something	
6	Belief the uncertainty in social media activities	Alternative thinker	Managing advertisement	
7	Seeking verification before proceed	Never underestimate	Managing perception	
8	Just delete the unnecessary		Understanding of process	
9	Changing the setting		Clear trace of activity	
10	Logout for every application		Early evaluation before action	
11	Password combination of more than 8 characters		No rushing	
12	Responsible for reporting unusual activities		Managing multiple website	
13	Recognition about something		Managing password	
14	Refusal		Managing inappropriate content	
15	Spontaneous decision making			
16	Clear trace after use			
17	Shut or close the pop-up screen			
18	Use anonymous name for online gaming.			

Figure 5.7: List of Initial Themes and its Sub-themes

iv) Reviewing themes

Step 4 involved reviewing the themes gathered from the previous step. In this step, the initial themes were checked against its relationship to personal data protection. This was to ensure that only themes and sub-themes which were related to personal data protection are remained. The themes and sub-themes were also checked against redundancy, and then rearranged and renamed accordingly. The outcome from this step was the list of final themes and its sub-themes as depicted in Figure 5.8.

Themes	Sub themes	Real interview scripts	List of participants ID	Related Literature Review
Desired behavior Definition: Good behavior which result in positive outcome.	**Password – Creation of password must be long and having combination of characters. (derived from quantitative study & observation) - Definition:** A combination of characters to be used for verification online application. **Thinking – Belief the uncertainty, think before act, refusal Definition:** The act of producing thought about something. **Trust – Common sense, Do not trust outsider and strangers, privacy Definition:** Degree of reliance about something.	"The thing is we need to meet them outside and they give their Facebook then only we can accept" "First of all I won't open the email. Because I won't recognized them" "He is opening multiple web pages inclusive of YouTube, Facebook, and Twitter and online shopping at the same time. He forgot to logout his twitter. Opening multiple web page make you forget to logout especially when you are rushing" "I'll only accept the one that I know	Y3, Y4, Y6, Y9, Y12	*"Prior work has shown that password-composition policies requiring more characters or more character classes can improve resistance to automated guessing attacks, many passwords that meet common policies remain vulnerable"* (Ur et al. 2013) *"System administrators typically require that users select passwords according to a password-composition policy designed to make users' passwords harder to predict. Such a policy may require, for example, that passwords exceed a minimum length, that they contain uppercase letters and symbols, and that they do not contain dictionary words"* (Komanduri et al. 2011) *"It feels heartless to think that way when you know some of the nice sorts of techies who thrive in our computation centric times. But we have to do our best at thinking dark thoughts if we are to have any forethought about technology at all"* (Lanier, 2013) *"An individual (trustor) will therefore concentrate on a limited set of information cues – including trust signals from the technology service (trustee) – which are important or relevant to them, to ascertain the ability and motivation (or willingness) of the trustee to safeguard their personal information"* (Morton, 2014

Figure 5.8: Sample of Defining Themes

v) Defining and naming themes

In this step, the initial themes was managed to be reduced and the finalised themes were derived. For each theme and sub-themes (please see Appendix Q), its definition, real quotation from interview script, participants' ID and related literature were given. This is to provide consistency and evidence in order to ensure validity of the theme selected. The finalised themes were, firstly, desired behaviour and its sub-themes include password, thinking, trust, information security actions and responsibility. The second theme was security culture and its sub-themes include never underestimate, self-realisation of harmful effect, differentiate between legitimate and illegitimate, and reliability. The third identified theme was program content and its sub-themes include management of discovery will, social interaction, information sharing, management of password and understanding processes involved in online activities. The final main theme derived was assessment component and it sub-themes include Internet literacy.

vi) Producing a report.

The final step was to produce a complete analysis report of the data collected for the interview. Thus, this section briefly reports the processes involved.

5.10 DISCUSSION ON THE FINDINGS AND CHAPTER SUMMARY

This chapter has presented the findings from the survey, pre-test and post-test surveys, observation of web recording and focus group interview conducted among youngsters who attended cybersecurity awareness program by Cybersecurity Malaysia. The data analysis for data collection Phase 1 (survey) was analysed using Multiple Regression in SPSS, data collection Phase 2 (pre-test and post-test) was analysed using the Wilcoxon test in SPSS. For the qualitative data collected through observation of web recording and interview, both were analysed using thematic analysis. In general, the findings is depicted in Figure 5.9.

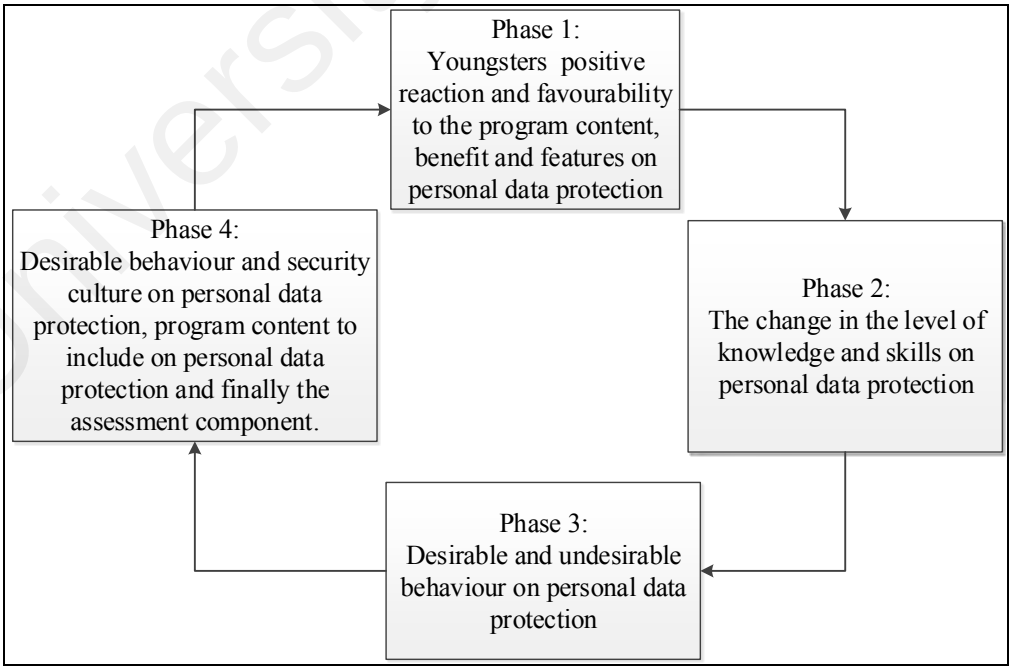

Figure 5.9: Summary of findings based on four phases

The finding from Phase 1 showed overall positive feedback among youngsters with regard to program contents, features and benefits on personal data protection. The finding from Phase 2 shows that there was a change in the youngsters' knowledge and skills but no changes were recorded for attitude. This may be due to the requirement and longer time needed to continuously educate and develop attitude among youngsters to protect their personal data. The finding from Phase 3 showed two important themes which were undesirable behaviour and desirable behaviour among participants. For undesirable behaviour, the sub-themes were same password used for multiple applications, no restriction in browsing the Internet, not clearing trace after using the Internet and lack of judgement. For desirable behaviour, the sub-themes were clearing trace after using the Internet, different and long password used, using anonymous name for username and closing the pop-up screen. The last finding based for Phase 4 was four main themes and its sub-themes. First was desired behaviour and its sub-themes included password, thinking, trust, information security actions and responsibility. The second theme was security culture and its sub-themes included never underestimate, self-realisation of harmful effect, differentiate between legitimate and illegitimate, and reliability. The next identified theme was program content and its sub-themes included management of discovery will, social interaction, information sharing, management of password and understanding processes involved in online activities. The final main theme derived was assessment component and it sub-themes included Internet literacy and parental guides, and control.

This study used Sequential Explanatory Design as a mixed method approach in data collection, data analysis as well as findings as discussed in Section 4.3. Therefore it is required to mix the findings and offer a brief discussion before it is used further to provide answers to the research questions.

Youngsters were found to have positive reaction to the program contents, benefits and features on personal data protection. However, the investigation based on their attitude reported no significant changes. This highlights the requirement to improve the current state of the cybersecurity awareness program to ensure changes in attitude. This statement is supported by findings on the observation of web recording which were consistent with the findings on attitude. In the findings on the observation of web recording, there were some undesirable behaviours among youngsters reported which highlight a need to make modifications to the current state of the cybersecurity awareness program to include important information in order to minimise undesirable behaviour. The desired behaviour and security culture through the findings from observation of web recording and focus group interview supported the findings on change in knowledge and skills. In addition, from the findings on reaction, youngsters were found to practise and know how to protect personal data. However, in comparison with findings from the focus group interview, youngsters were found to underestimate, have little self-realisation on harmful effects and lack the ability to differentiate between legitimate and illegitimate aspects in the digital world. This statement is supported by the findings on the focus group interview. Youngsters require guidance in terms of management of their discovery will, social interaction, and management of password and understanding process involved during online activities.

Overall, findings suggest the assessment of the cybersecurity awareness program on personal data protection is able to gain feedback from youngsters. However, in order to accommodate the new growing technologies that use Internet as a medium, it is a requirement to improve the current state of the cybersecurity awareness program. Among the proposed improvement is to include the aspect of decision making as part of the awareness as well as management of password, online application and online

content. There is some level of agreement with this proposal among experts from Cybersecurity Malaysia who were invited to validate the findings. The following Chapter 6 provide discussions and conclusion to the overall research. Specifically, an overview of the research is provided. The findings from the youngsters will be related to the formulated research questions posed in Chapter 1. The next chapter also includes discussion as a way to provide insights from the literature and from the theoretical perspective. Contributions to the body of knowledge by this study to theory and practice will be highlighted. Furthermore, next chapter also discusses the limitations of this study and proposes areas for future research study.

CHAPTER 6

DISCUSSION AND CONCLUSION

6.1 INTRODUCTION

The general objective of this study was to explore and use a systematic technique in performing assessment of a cybersecurity awareness program among youngsters with regard to their understanding on personal data protection. Specifically, the objectives of this study were i) to identify the assessment criteria's for cybersecurity awareness program based on theories and component of personal data protection ii) to propose an assessment framework for cybersecurity awareness program iii) to employ the proposed assessment framework for assessing cybersecurity awareness program among youngsters and iv) to verify the proposed assessment framework for cybersecurity awareness program.

This study is important due to several research gaps identified in the existing literature concerning: (a) few attempts found from the literature that used systematic evaluation technique in assessing cybersecurity awareness programs (Caputo, Pfleeger, Freeman, & Johnson, 2014; Aggeliki Tsohou et al., 2008), (b) lack of studies that focused on assessment of cybersecurity awareness programs among youngsters (Sithira & Nguwi, 2014; Livingstone et al., 2005; Johansson & Götestam, 2004) and (c) lack of studies in assessing the cybersecurity awareness program focusing on personal data protection (Broadhurst & Chang, 2012; Aimeur & Schonfeld, 2011).

In order to address the identified research gaps, empirical data collection was carried out. This study was designed using a mixed method strategy named Sequential Explanatory Design. The data collection process was conducted in four sequential phases. In Phase 1, a survey was used as the instrument with an aim to measure the youngsters' reaction towards the cybersecurity awareness program content, features and benefits. In Phase 2, pre-test and post-test surveys were used as instruments which aimed to measure the changes in knowledge skills and attitude among youngsters after attending cybersecurity awareness program. In Phase 3, observation of web recording was used as an instrument with an aim to observe youngsters' behaviour as they browsed the Internet. In Phase 4, a focus group interview was used as an instrument with an aim to measure the result and impact of the cybersecurity awareness program among youngsters. The data collections were held at two OUTREACH CyberSAFE programs conducted by Cybersecurity Malaysia.

Several findings were obtained from this study. The analysis done for data collection Phase 1 found that youngsters had a positive reaction towards the program content, features and benefit. In Phase 2, knowledge and skills of youngsters had changed. However, no changes were reported in the youngsters' attitude after attending the cybersecurity awareness program. Since this study used Sequential Explanatory Design as the mixed method approach, the data was first collected via a quantitative approach in Phase 1 and Phase 2, and then were combined with the findings gained from the data collection in Phase 3 and Phase 4. In Phase 3 and Phase 4, findings gained were in the form of themes and its sub-themes. The themes found in Phase 3 were in terms of the desirable and undesirable behaviour observed among youngsters. In Phase 4, the finding was desired behaviour, security culture, and program content and assessment components. In the following section, the findings mentioned were used to answer the

research questions from the findings which were integrated and mixed from each of the phases involved.

6.2 DISCUSSION OF RESULTS AND ANSWERS TO RESEARCH QUESTIONS

The following subsection discusses in more detail about the results in terms of answers for each research questions presented earlier in this thesis. The answers were derived from the findings mentioned in Chapter 5. The discussion also relates to the literature and theoretical linkages used in this study.

6.2.1 Research Question One – "What are the identified assessment criteria's for cybersecurity awareness program based on program evaluation model and component of personal data protection?"

The aim of research question was to identify the assessment criteria's based on the reviewed theories and components of personal data protection. The purpose of this identification is to provide the groundwork to select the appropriate program evaluation technique that is used to develop the assessment framework for cybersecurity awareness program. The developed framework is discussed later in the following subsection. Several assessment criteria's are identified through literature search.

The first step in answering this research question is reviewing on components of personal data protection. As suggested by (Madden et al., 2013; Livingstone et al., 2005), the components of personal data protection that related to youngsters mainly focus on password management, the usage of social technologies and concern over

privacy. For each one of the components a comprehensive review was made. According to literatures (Amanda Lenhart, 2015; Amanda Lenhart et al., 2010), password management is crucial among youngsters as they often use simple password and share it among family and friends. This is consistence with Kaye, (2011) and Singh et al., (2007) findings during data collection. The youngsters use simple password that can easily be remembered such as their birth date, identification number and sometimes their real name. Since the usage of social technologies among youngsters is emerged today, it raises concerns on the usage of their personal data. As social media widely connected users regardless of their geographical boundary, it opens great range of opportunities for the third party to steal and misuse the personal data placed by the youngsters. The suggestion to include the usage of social technologies is made according to the statement made by (Madden et al., 2013; Lenhart et al., 2011; Livingstone et al., 2005). Last but not least, the component of personal data protection is concerning on privacy. Ignorance among youngsters often results in their lack of concern over privacy thus this is another door for third party to invade them (Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee et al., 2012). Considering these three important components, the proposed conceptual framework is developed accordingly by incorporating these components.

The second step in answering this research question is to review the relevant theories. In this studies the following theories were reviewed, ARCS, SLT and TRA. The components of assessment suggested in this theory were carefully reviewed and the following suggested assessment criteria are identified; (1) Motivational: Attention, Relevance, Confidence and Satisfaction, (2) Learning: Content, Activity and Culture, (3) Behaviour: Attitude towards acts, Subjective norm and Behavioural Intention. The reviewed made upon several theories is to ensure appropriate selection of program

evaluation model used in this study. Each of these identified assessment criteria's were check against several program evaluation models as mentioned in the previous section 3.8. Kirkpatrick Four Learning Evaluation Model is nominated as the guideline to propose assessment framework for cybersecurity awareness program as it include the assessment on reaction, learning, behaviour and result.

6.2.2 Research Question Two – "What is the proposed assessment framework for cybersecurity awareness program?"

The aim of research question two was to propose an assessment framework for cybersecurity awareness program. In this study, a nominated program evaluation model called the Kirkpatrick's Four Learning Evaluation Model is used. In the exploration of using Kirkpatrick's Four Learning Evaluation Model, a comprehensive understanding on the cybersecurity awareness program on data protection was revealed based on findings derived from the four components of assessment. This statement is consistent with suggestion by Abawajy et al. (2008), who stated that the program evaluation model could be explored in assessing and analysing the cybersecurity awareness program effectiveness.

In this study, Kirkpatrick's Four Learning Evaluation Model was used as conceptual framework by focusing on four assessment components, as follows; reaction, learning, behaviour and result. The components were meant to understand the cybersecurity awareness program on personal data protection. The components used in each level of assessment were different as opposed to previous assessments on cybersecurity awareness programs which mainly focused on single components such as identifying experience, usage of security measure, attitude while accessing the Internet and security

perception, as in studies conducted by Furnell et al. (2008) and Furnell, Bryant, & Phippen (2007). The approach in Kirkpatrick's Four Learning Evaluation Model was different, where some of components have opened flexibility in terms of choosing methodologies in order to best suit the data collection for each component. In this study, mixed methodology approach through Sequential Explanatory Design was used to perform an empirical study. This is in contrast to the previous approach in assessing cybersecurity awareness programs which mainly considered single methodology for assessing a component such as behaviour without looking at other components of assessment according to Kirkpatrick's Four Learning Evaluation Model (Ng et al., 2009; Stanton et al., 2005). By having a single methodology in assessing cybersecurity awareness programs among youngsters, it may suffer from achieving incomplete information and biasness. This is consistent with Schmidt & Hunter (2014) and Podsakoff, MacKenzie, & Podsakoff (2012) who claimed that bias may be derived from a single measurement criterion. In this study, the finding derived from the survey, pre-test and post-test surveys, were mixed and compared in order to reveal the actual findings on the understanding of the cybersecurity awareness program. For instance, in an assessment conducted for reaction, majority of the participants gave positive feedback on their understanding on personal data protection. However, the findings from an interview showed a different result whereby youngsters were found that they require guidance in terms of managing their passwords and making decisions on their usage of personal data. This finding is consistent with Bates (2004) who acknowledged Kirkpatrick's Four Learning Model as a way to identify valuable or descriptive information across components which can ensure the findings quality and consistency. Furthermore, Kirkpatrick's Four Learning Evaluation Model has provided a rich context for understanding the impact of the cybersecurity awareness program on personal data

protection which is more specific, differentiated and useful for any change and adjustment required (Praslova, 2010).

Although this study did not cover the entire series of cybersecurity awareness programs conducted by Cybersecurity Malaysia, the use of Kirkpatrick's Four Learning Model however bears several beneficial findings. The findings derived from the assessment could be extended to stakeholders such as CSM, parents, management of schools and responsible institutions for conducting cybersecurity awareness programs. The establishment of an assessment model that can cater for a great number of participants was highlighted by Mertens (2014) who mentioned that programs involving a large number of participants require a systematic approach in investigating the program. The application Kirkpatrick's Four Learning Evaluation Model in previous study by Ahmad, Johnson, & Storer (2015) was successful in conducting an assessment on a large scale cyber exercise that was used to simulate cyber incident environments in order to assess the knowledge and skills of information security personnel. The exploration and use of Kirkpatrick's Four Learning Evaluation Model has resulted in ensuring the validity of input given by the youngsters. For example, in a case where only a survey was used to gain feedback, it may not fully represent views from the youngsters who have a higher tendency to give incorrect feedback. However, by using Kirkpatrick's Four Learning Evaluation Model which comprises of different levels of assessments and methodologies, the degree of validity increased. This is because the analysis is conducted based on the combined information gathered from the different methodologies used. This is supported by Kirkpatrick (2009) who stated that the Kirkpatrick Model is able to ensure validity of findings.

In the aspect of analysing human behaviour, conclusion cannot be made on only a single perspective such as observation. Human behaviour is complex to understand as it involves the information on capacity of mental, physical, emotional and social. Therefore, assessment through Kirkpatrick's Model is found to be suitable as it consists of different components of assessment where different findings could be revealed. In this study, findings from assessing the youngsters' behaviour from observation of web recording is supported by findings gained through the focus interview session. To a certain degree, youngsters were found pretending while they were being watched but through the focus group interview session, their statements were contradicting. This statement is in line with Carter (2013) who claimed that analysis of human complex behaviour requires a systematic approach. As this study specifically involved youngsters, the assessment had to be conducted in a systematic way to allow not only systematic but an in-depth approach. This is aligned with the approach to assess youngsters as suggested by Barbovschi & Marinescu (2013) and Ólafsson (2013) who claimed that proper planning is required prior assessment is conducted which involves youngsters and the selection of research design must be able to tackle the observed scenarios.

Based on the general findings from this study, Kirkpatrcik's Four Learning Model was found to be able to propose a decision as to include improvements to the current cybersecurity awareness program. Accordingly, this decision was supported by Cybersecurity Malaysia. This conclusion was fully appreciated by an expert panel from Cybersecurity Malaysia. Based on the above discussion and justification, it was proposed that Kirkpatrick's Four Learning Evaluation Model to be used as the assessment framework on personal data protection.

6.2.3 Research Question Three –"How to employ the proposed framework for assessing cybersecurity awareness program among youngsters?"

Research question three was designed to meet the following research objectives i) to employ the proposed assessment framework for assessing cybersecurity awareness program among youngsters and ii) to verify the proposed assessment framework for cybersecurity awareness program. Boyd (2007), Livingstone et al. (2005) and Johansson & Götestam (2004) stated that the study on youngsters at specific age segment was important because they were found in a state of potentially exhibiting addictive behaviour towards online technology and Internet applications as well as lack in security practice that can protect them from Internet vulnerabilities.

In order to provide an answer to research question number three, the propose conceptual framework based on Kirkpatrick Four Learning Evaluation Model is used to facilitate and design the instruments, data collection steps and data analysis technique involved. The purpose of research question three is to ensure the proposed conceptual framework is practical to be used among youngsters. The employment of proposed conceptual framework is observed by looking at the findings taken from each data analysis phase, and its capability to mix and provides understanding of the cybersecurity awareness program among youngsters. The initial findings gained from the youngsters through surveys were encouraging with regard to the program content, features and benefit on personal data protection. However, questions were raised as to what extent this positive finding translated into their actions in protecting their personal data. This is consistent with an argument made by Barbovschi & Marinescu (2013) and Atkinson et al. (2009) who were concerned about the practical aspect of personal data security among youngsters. According to them, youngsters often neglect the importance of protecting

their personal data as they were very enthusiastic in using the Internet. Similarly, the findings from the assessment conducted discovered that youngsters sometimes share passwords among their peers and family members. In addition, they were rushing in making decisions while browsing the Internet.

There was another component that was assessed in this study, which was the learning outcome after attending the cybersecurity awareness program. Assessment on learning outcome among youngsters specifically targeted to measure changes in knowledge, skills and attitude. In this study, it was found through the pre-test and post-test surveys that youngsters' knowledge and skills had increased as opposed to their attitude. It can be claimed that this finding was consistent with past research pertaining to youngsters' learning outcome as in a study conducted by Fitton, Ahmedani, Harold, & Shifflet (2013) who recorded that changes occurred among adolescents' knowledge and skills in terms of technology usage. In the context of attitude that have no changes in this study, it is believed that to have changes that occurred in knowledge and skills, a long span of time and continuous effort are required to give awareness on personal data protection among youngsters. This is because changes in attitude are a complex process as claimed by Vogel & Wanke (2016). Furthermore, this finding is supported by Bada & Sasse (2014) who investigated attitude and found challenges in improving information security behaviours. The main reason is because changing an attitude requires more than giving awareness on risk and positive attitude but also concerns on the ability and willingness of an individual to understand and apply the awareness gained. In this study, the findings in attitude were supported by the findings gained through the observation of web recording. It was revealed that after analysis was done on the observation data, there were lists of desirable and undesirable behaviour recorded among the participants. Thus, based on the observation of web recording findings, youngsters who were found

to have changes in knowledge and skills also had undesirable behaviour such as having the same password used for multiple applications, no restriction in browsing the Internet, not clearing the trace after using the Internet and lack of judgement. An interesting finding discovered during the observation of web recording, it was revealed that the youngsters sometimes tried to be secretive while they were being watched. This explains the same scenario in a situation when their parent was around. This additional finding supported by a study done by Smahel et al. (2012) on excessive internet use among European children which found that children were pretending with their online activities if they were being watched or asked by their parents.

The understanding of cybersecurity awareness program was further investigated through the focus group interviews which discovered findings focusing on desirable behaviour, security culture practices among youngsters, program content and assessment components. The findings showed that youngsters practise desirable behaviour such as having long password and their trusts were given after judgement made on positive and negative consequences. Similarly, in the perspective of security culture, it was found that youngsters had given extra precaution and always thought about negative consequences prior to making decisions. However, in comparison to the undesirable behaviour observed and revealed from the focus group interview, youngsters require extra guidance as they must overcome their oversharing attitude as mentioned by Furnell (2010), Livingstone et al. (2005). Finally, this research provided evidence that the proposed conceptual framework is practical and its findings were able to generate the understanding of cybersecurity awareness program among youngsters on personal data protection.

However, to ensure the practicality of the proposed assessment framework it requires verification by the panel expert. Thus the next step to answer this research questions is to make verification with panel expert. Verification mentioned here composed of the propose framework and suggestion for improvement. The panel experts are officers who involve in managing and conducting cybersecurity awareness program in Malaysia.

Throughout the findings analysis, there were improvements and emerging components which were found to be suitable to be proposed in order to ensure youngsters were fully equipped on personal data protection. This suggestion of improvement and emerging components is used to verify the practicality of conceptual framework. The feedback from panel expert is depicted in Appendix N and O. The proposed enhancement components were made based on the understanding derived from the research findings. In previous assessments, personal data protection was not given a focus as most assessments of cybersecurity awareness programs were concerned with understanding security in general without specifically emphasising on personal data protection as in line with the assessment conducted by Kim (2014), Mani et al. (2014) and Furman et al. (2012). By focusing on personal data protection during the assessment, this study found evidences on components of personal data protection that require attention from stakeholders such as CSM, parents, management of schools and institutions that are responsible in conducting cybersecurity awareness among youngsters. The proposal for enhancement components with regard to personal data protection was motivated by present problems and concerns over protecting personal data as highlighted in Hong & Thong (2013) and Young & Quan-Haase (2013). A lack in personal data protection was found to be among the cause of cyber threat problems among youngsters. By empirically investigating the current state of the cybersecurity awareness program through the assessment conducted in measuring youngsters' reaction, learning,

behaviour and result, this study proposed enhancement to the current cybersecurity awareness module which specifically focused on personal data protection. Throughout the analysis, by comparing result in each phases of data collection, the following emerged components are derived. Each emerged component was discussed one by one together with its supporting literatures support and justification.

i) Decision making process in using personal data

The requirement to educate youngsters on the decision making process in the cybersecurity awareness program is deemed necessary to minimise the risk of their personal data being exposed to third parties. The proposal to educate youngsters on the decision making process in using personal data is in alignment with various literatures that are concerned on the capacity of youngsters or adolescents in making matured decision. Albert, Chein, & Steinberg (2013), LaRose, Lin, & Eastin (2003) and Steinberg & Cauffman (1996) specifically suggested that youngsters require guidance in their Internet usage as they were found to be lacking in self-regulation. This proposed enhancement was consistent with findings recorded during the focus group interview session which revealed youngsters are lacking in judgement especially in differentiating between legitimate and illegitimate applications available over the web. Initial judgement and individual evaluation is important to be stressed on during the cybersecurity awareness program because it helps to increase the cognitive process among youngsters to think more than once and realise the negative consequences of their decision. This statement is supported by Livingstone et al. (2005) who mentioned that youngsters are in the process of building their cognitive ability which requires continuous guidance in order to increase their degree of maturity. However, the current cybersecurity awareness program module does not include decision making as part of the cybersecurity awareness content. This proposed enhancement component was

acknowledged by CSM as it could add value to their current module used to convey the message on personal data protection among youngsters in Malaysia (please see Appendix N and O). Practically, by adding decision making process as part of the cybersecurity awareness message, youngsters could have insights on how better decisions could be made on filtering and sharing their personal data in digital world.

ii) Management of online application

Based on the survey conducted in this study, youngsters were found to be actively using the Internet for social media, email, watching online videos and also for downloading songs, drama, films and software. The confirmation of various Internet applications used among youngsters is supported based on the findings from the focus group interview. It was found that the majority of youngsters who participated in this study had at least one social media account. In accordance to Acquisti et al. (2015) and Spiekermann et al. (2015), social media has given tremendous impact on personal data protection as it involved extensive use of personal data. Additionally, Lenhart et al. (2011) mentioned that youngsters often left their digital footprint available on the web. Furthermore, Lenhart (2012) added that the usage of smartphone devices gave youngsters an easy platform to access their online social media account. Even though the findings in this study confirm youngsters as skilful and advanced Internet users, they need to be educated on the aspect of managing their online applications. This is because as mentioned by Joe & Ramakrishnan (2014), online social media provide an unsafe environment as personal data were made to be online and publicly available to the public. This could encourage cyber criminals to steal details of youngsters' social media accounts and use it to hack other online applications used by the same users. The proposal of enhancement components on the management of online activities is supported by Correa et al. (2013) who claimed that youngsters shall be made to know

how in managing their online applications and determine the authenticity of applications that they used in order to minimise their personal data from being stolen. Therefore, this study contributes in making suggestions to improve the current cybersecurity awareness module by including awareness on how to manage online applications used by youngsters. For instance, education on which type of personal data could be revealed and how it is prompted by online application.

iii) Management of online contents

The next enhancement component proposed is to include management of online content among youngsters. Based on the understanding conducted on the observation of web recording, youngsters were found to have freedom while browsing the Internet. Similarly, the finding from the interview showed that there were youngsters who claimed that they could freely browse Internet without supervision by their parents. Online content could sometimes be tricky and require judgement from the youngsters on which content is applicable to them as the Internet contains inappropriate content and advertisements which sometimes prompt them to provide their personal data (O'Keeffe et al., 2011; De Moor et al., 2008). Because of the free availability of the content, youngsters often browse without thinking that the content can lead to harmful effects on their personal data. Due to this reason, this study proposes to include the management of online content in order to assist youngsters to differentiate between appropriate and inappropriate content. This suggestion is aligned with Valcke, De Wever, Van Keer, & Schellens (2011) who performed longitudinal study on the nature of internet usage and parental supervision among young children and stressed the importance to educate young Internet users on the content.

iv) Management of password and username

The importance of protecting passwords and usernames from being stolen and used by third parties should be made clear to the youngsters. This includes characteristics of a good password, where a combination of characters symbols and numbers that can produce good passwords. This also includes policy of passwords sharing. It could be observed from the findings that there were youngsters who used simple passwords and admitted sharing passwords among their friends and family. In addition, there were also youngsters who chose to paste their passwords at places that could be easily remembered. All these actions were found to have potential risk to their personal data. Therefore, it is proposed to include knowledge on how to protect their password as well as to avoid using their full name for the username. This suggestion is consistent with Vandoninck et al. (2014), Smahel et al. (2012) and Lenhart et al. (2011) who highlighted the need for education on password management among youngsters as a way to protect their personal data from being unintentionally revealed to strangers. For that reason, this study reinforces the need to include management of passwords and usernames as part of the cybersecurity awareness program.

6.3 REVISITING CONCEPTUAL MODEL

The conceptual framework discussed in Chapter 3 (refer to section 3.10) integrate the concept from the literature, reviewed theories and adopted assessment model of Kirkpatrick's Four Learning Evaluation Model. The conceptual framework formed a guideline for the research design, how the research is conducted, including data collection procedures as well as data analysis. Based on the findings, some modifications were proposed to be made to the earlier conceptual framework, as in

Figure 6.1. The revised conceptual framework, for use in future studies on assessment of cybersecurity awareness programs, is composed of the following elements:

i) Subject: Youngsters and stakeholders such as CSM, parents and responsible organisations providing security awareness sessions.

ii) Data Source: Youngsters' feedback after attending the cybersecurity awareness program.

iii) Component of assessment

a) Level 1 – Assessment on participant reaction

b) Level 2 – Assessment on level of learning

c) Level 3 – Assessment on change in behaviour

d) Level 4 – Assessment on the result

iv) Assessment Result: Analysed feedback given by youngsters

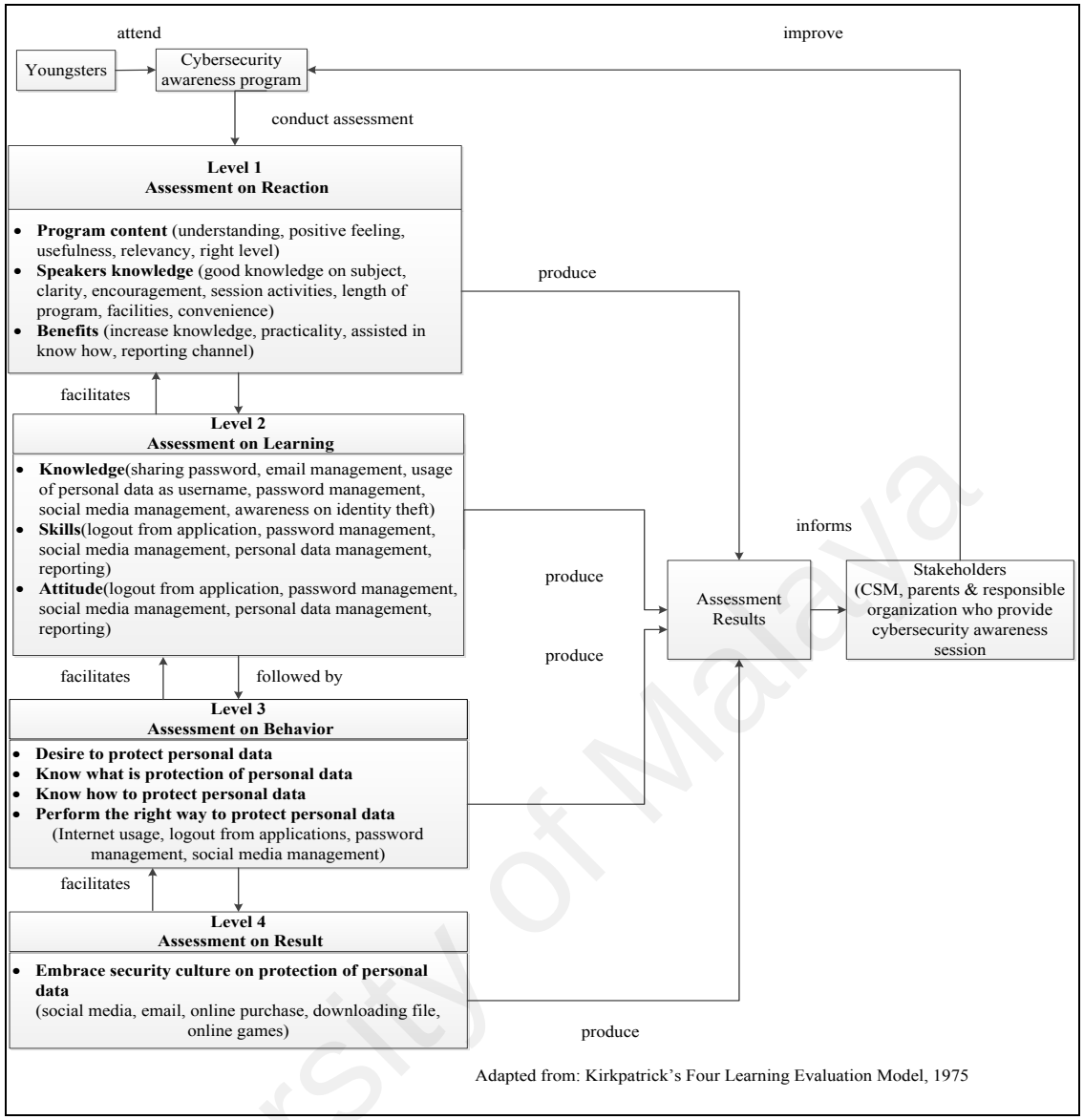

Figure 6.1: Cybersecurity Awareness Program Assessments Framework on Personal Data Protection

The research findings in this study generally enhance the original conceptual model that used Kirkpatrick's Four Learning Evaluation Model for conducting assessment. For example, in the original Kirkpatrick Model, there were only four assessment components used in performing the assessment on personal data protection among youngsters. However, as this study is conducted, the construction of Kirkpatrick Four Learning Evaluation Model is modified by incorporating the elements of personal data protection and its usage to individually assess the youngsters. The execution of each

assessment level is required in order to ensure concrete assessment results. The assessment result will be made known to the stakeholders and a decision will be made whether or not to include the propose enhancements and improvements.

6.4 RESEARCH CONTRIBUTION

This study has made a number of research contributions to the existing knowledge on the assessment of cybersecurity awareness programs on personal data protection by identifying assessment criteria's, using a more systematic assessment method, incorporating an age segment that was often disregarded during previous assessments and specific scope of assessment focused on personal data protection. The research contributions made are as the following.

Identified assessment criteria are based on the reviewed theories and components of personal data protection.

Based on the theories and components of personal data protection reviewed, the identified assessment criteria's is revealed. This has provided a strong foundation in proposing the conceptual framework of assessing cybersecurity awareness program among youngsters in Malaysia. The identification of assessment criteria's also ensuring initial systematic approach is used to nominate the appropriate program evaluation model.

The use of a systematic approach taken from program evaluation technique to assess the cybersecurity awareness program.

Using a systematic approach in making an assessment, various levels of assessments could be made and recorded. The result of using the systematic approach is beneficial to the stakeholders and responsible organisations that provide cybersecurity awareness programs, trainings and sessions. The extended benefit of using the systematic approach is that it could assist in decision making by the stakeholders on whether to continue, suspend or add new modules as required. Previous assessments used mainly straightforward methodologies which limit the findings to be from only one component. However, by using different components of assessment, this study allowed various feedbacks to be analysed systematically.

Assessment result that provide insight to stakeholders in terms of the cybersecurity program among youngsters.

The assessment result produced in this study provided insights to stakeholders such as CSM, parents and organisations responsible in providing security awareness sessions with regard to the understanding of cybersecurity awareness among youngsters. Previously, little concern was given to assess youngsters. Therefore, conducting this study extended the previous scope of assessment which merely focused on assessing adults. The insights given by this study is important in assisting stakeholders in making decisions as well as planning for the improvement of the current state of the cybersecurity awareness program for educating youngsters.

Identified components of personal data protection to be highlighted to the youngsters

Educating youngsters has always been challenging due to their desire to explore and use Internet technology. Thus, it is important to equip them with the knowledge on how to protect them in the Internet environment. As this study was concerned with protecting personal data, it has been proposed, based on the research findings, that there were elements which require more attention and focus in educating youngsters. Therefore, this study is deemed beneficial as an extractor to find and dig information from the youngsters.

6.5 RESEARCH IMPLICATIONS

The research implications can be seen from the development of the conceptual framework in the earlier chapter of this thesis and its subsequent revision. The outcomes of this study have brought an additional aspect of knowledge based on the empirical investigation related to the assessment of cybersecurity awareness program on personal data protection among youngsters. The research implication is explained by the potential theoretical and practical implication.

6.5.1 Theoretical Implication

The use of ARCS Model of Motivational Design Theory, Situated Learning Theory and Theory of Reasoned Action to identified assessment criteria's to nominate appropriate program evaluation model.

The adaption of ARCS Model of Motivational Design Theory, Situated Learning Theory and Theory of Reasoned Action has formed the theoretical perspectives on how

to conduct this study. It also has provided significant foundation is developing the conceptual framework. The review made upon the theories revealed, suggested that assessment criteria's must be conducted in order to ensure comprehensive assessment on the respondents.

The use of Kirkpatrick's Four Learning Evaluation Model

The adaption of Kirkpatrick's Four Learning Evaluation Model as an appropriate program evaluation model is more personalised compared to other relevant model particularly in studying youngsters because it has different levels of assessments concerning towards investigating the valid feedback. Each level of assessment complements each other and produces valid feedback to be used for analysis. The conceptual framework that was developed based on the identified assessments criteria's that nominated Kirkpatrick's Four Learning Evaluation Model, with additional consideration to incorporate components of personal data protection has resulted in a subsequent revision to the original Kirkpatrick's Four Learning Evaluation Model. By linking the Kirkpatrick's Four Learning Evaluation Model with the components of personal data protection, the assessment provides further understanding on the effectiveness of the current module used to conduct the cybersecurity awareness program. This research has enriched the utilisation of Kirkpatrick's Four Learning Evaluation Model which was previously used in the context of assessing education programs.

6.5.2 Practical Implication

Proposal of a framework to assess cybersecurity awareness programs

A framework that can be applied to assess cybersecurity awareness programs is proposed based on the findings from this study. The framework consists of four levels of assessment components which are assessment on reaction, learning, behaviour and learning. All of these levels have been described accordingly. The purpose of this framework is to provide a more systematic approach in conducting assessments of cybersecurity awareness programs.

Extension of program evaluation technique that was previously less considered in assessing cybersecurity awareness programs.

Kirkpatrick's Four Learning Evaluation Model has benefited the education field as well as the medical field. A number of assessments have utilised this program evaluation technique and improvement has been made to the current state of the program. On this basis, the selection of using Kirkpatrick's Four Learning Evaluation Model is extended for application in assessing cybersecurity awareness programs.

A clearer understanding of youngster feedback on personal data protection

The outcome of this study has resulted in a clearer understanding of youngster's feedback on personal data protection. This feedback is beneficial in explaining the current understanding among youngsters on personal data protection and determining whether youngsters cultivate a security culture in protecting their personal data.

Facilitate stakeholder to decide or plan for a better module to convey the message on personal data protection to youngsters.

The outcome from this study has suggested improvements to be made to the current cybersecurity awareness module used by CSM in educating youngsters particularly on personal data protection. Improvement suggested can facilitate stakeholders, in particular CSM, in deciding and planning for a better module for the cybersecurity awareness program on personal data protection.

Experience of conducting evidence-based research

This research was conducted based on real-life experiences and evidence of youngsters who attended cybersecurity awareness program. Thus, it contributed to enhance the quality of empirical research results that were beneficial for stakeholders such as CSM, parents and organisations responsible in conducting cybersecurity awareness programs. By gathering data from two different real-life cybersecurity awareness programs, the scope of this research had been broadened and allowed for comparison of data sources. However, the empirical evidence in this study was based on combined data gathered from both cybersecurity awareness programs. It was an effort to bridge both theory and practice pertaining to the assessment on cybersecurity awareness programs as shown by the literature review.

6.6 RESEARCH LIMITATIONS

A number of research limitations were observed throughout this study. Thus, it shall be acknowledged in order to provide better research avenues for future works. The research limitations are briefly described as follows:

i) The focus group interview and observation of web recording sample size was limited to 12 participants from the total participants of the cybersecurity awareness program. Although this might not be considered in representing a sample and be generalized, the study generated useful data and gave better insights on the cybersecurity awareness program. This is because this study was designed based on the mixed method approach in which the data collected through the focus group interview and observation of web recording were merged with data derived from surveys, pre-test and post-test surveys. Through the research design, data from the focus group interview and observation of web recording provided contrasting context that explained the data gathered from the survey and the pre-test and post-test surveys.

ii) The selection of participants was limited to those who attended the OUTREACH-CyberSAFE (cybersecurity awareness program) conducted by Cybersecurity Malaysia only. No other cybersecurity awareness programs or organisations were involved.

iii) Female respondents in Phase 1 and 2 are greater than male. However the nature of this study does not take gender as an influence factor but rather view the findings as collective.

iv) The instruments developed for this study was designed towards analysing the feedback and information pertaining to personal data protection only. It may not be significant in explaining the assessment of other different types of security issues.

6.7 FUTURE RESEARCH

Based on the limitations identified in the previous section, few areas warrant future research:

i) As the sample size used during focus group interview and observation of web recording was considered rather small, future studies could increase the sample size in order to make the findings more representative.

ii) A wider selection of participants from other cybersecurity awareness programs in other state and location conducted among youngsters. This would allow possible comparison of data sources and enhance the accuracy of empirical findings on the understanding of cybersecurity awareness programs among youngsters.

iii) Minimize gender bias opinion by ensuring approximately having equal number of respondents between male and female.

iv) An extension to the scope of this study by performing modifications to the developed instruments in order to perform assessment of cybersecurity awareness programs on different security issues for instance, privacy, information warfare and cyber harassment. The assessment on other security issues could enrich the findings on the effectiveness of the cybersecurity awareness program among youngsters.

6.8 SUMMARY

This chapter provides a conclusion to this research. It started by recapping the objective of this study, research gaps, methodology in data collection and the data that was

analysed. The discussion on findings was made around the circle of three research questions posed earlier in the research. The findings were discussed against the existing literature including recent works on the topic. By revisiting each research question, reflection on the findings were made. In general, the findings support and extend previous researches on the assessment of cybersecurity awareness programs. This research also made several contributions to knowledge and practice. These include the aspect of decision making in using personal data, management of online applications, online content and password. The conceptual framework proposed in the early part of this thesis was refined based on the findings gained in this study. The new conceptual model in the form of assessment framework for cybersecurity awareness programs provides a platform for future assessments. The next presentation in this chapter includes a brief identification and discussion on the theoretical and practical contributions. Although this study made a number of contributions, there were several recognized limitations. Suggestions were made towards addressing these limitations in future studies.

6.9 RESEARCH CONCLUSION

The main focus of this study was to perform an assessment on youngsters by getting their feedback after attending a cybersecurity awareness program by applying the proposed framework. The feedbacks recorded their reaction, learning outcomes, behaviour and results particularly on personal data protection. The study was carried out due to the fact that previous assessments were lacking in performing a systematic assessment, having little focus on youngsters and little emphasis on personal data protection. This study started with the development of the conceptual framework which guided the construction of instruments and sample selection. The real field work then

took place by systematically conducting a survey session, pre-test and post-test surveys, focus interview and observation of web recording session. It was done in sequence and data was collected and recorded. It was followed by a data analysis step for each type of data. The finding was built upon the results gained from quantitative and qualitative data analysis. Several conclusions were drawn from the steps taken. The topic addressed in this research is considered novel as it sought to perform systematic assessment on a cybersecurity awareness program particularly on youngsters. Multiple components of assessments offered a complete view and alternative findings on the effectiveness level of the current cybersecurity awareness module on personal data protection. This study also offered a novel way in assessing cybersecurity awareness programs by proposing an assessment framework that can be used and replicated in assessing other cybersecurity awareness programs. By identifying enhancement components on personal data protection to the current module of the cybersecurity awareness program, this study offered another novelty as this enhancement can be a valuable input for better modules. To sum up, the cybersecurity awareness program involving youngsters need to be continuously assessed and updated with new information as Internet technology evolves rapidly and offers new security risks from time to time.

REFERENCES

A'Campo, L. E. I., Spliethoff-Kamminga, N. G. A., Macht, M., The Edupark Consortium, & Roos, R. A. C. (2010). Caregiver education in Parkinson's disease: formative evaluation of a standardized program in seven European countries. *Quality of Life Research*, *19*(1), 55–64.

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248.

Abawajy, J., Thatcher, K., & Kim, T. (2008). Investigation of stakeholders commitment to information security awareness programs. In *2008 International Conference on Information Security and Assurance (isa 2008)* (pp. 472–476). IEEE.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514.

Aimeur, E., & Schonfeld, D. (2011). The ultimate invasion of privacy: Identity theft. In *2011 Ninth Annual International Conference on Privacy, Security and Trust* (pp. 24–31). IEEE.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action Control* (pp. 11–39). Springer Berlin Heidelberg.

Akhurst, J., & Lawson, S. (2013). Workforce innovation through mentoring: An action research approach to programme evaluation. *International Journal of Theraphy and Rehabilitation*, *20*(8), 410–416.

Al-Hamdani, W. a. (2006). Assessment of need and method of delivery for information security awareness program. *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development - InfoSecCD '06*, 102.

Albert, D., Chein, J., & Steinberg, L. (2013). The teenage brain peer influences on adolescent decision making. *Current Directions in Psychological Science*, *22*(2), 114–120.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, *26*(4), 276–289.

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, *42*, 56–65.

APNIC. (2004). *APNIC Annual report 2004*. Retrieved from https://www.apnic.net/__data/assets/pdf_file/0004/2668/2004AnnualReport.pdf

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312.

Ashenden, D. M. (2015). *Information security awareness: Improving current research and practice*. University College London.

Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud & Security*, (July), 13–19. B. Kim, E. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, *22*(1), 115–126.

Bada, M., & Sasse, A. (2014). *Cyber security awareness campaigns: Why do they fail to change behaviour?* Oxford, UK.

Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, *31*, 48–56.

Banjok, I., Puddester, D., MacDonals, C. J., Archibald, D., & Kuhl, D. (2012). Building posotive relationships in healthcare: Evaluation of the teams of interprofessional staff interprofessional education program. *Contemporary Nurse*, *42*(1), 76–89.

Barbovschi, M., & Marinescu, V. (2013). Youth. Revisiting policy dilemmas in internet safety in the context of children's rights. *Towards a better internet for children*, 227-246.

Beirness, D. J., & Beasley, E. E. (2014). An evaluation of immediate roadside prohibitions for drinking drivers in British Columbia: findings from roadside surveys. *Traffic Injury Prevention*, *15*(3), 228–233.

Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, M. M., Michelle L. Mazurek, Timothy Passaro, Richard Shay, T. V., & Lujo Bauer, Nicolas Christin, L. F. C. (2012). How does your password measure up? The effect of strength meters on password creation. In *21st USENIX Security Symposium (USENIX Security 12)* (pp. 65–80).

Boyd, D. (2007). Why Youth Heart Social Network Sites : The Role of Networked Publics in Teenage Social Life, *7641*.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*, 77–101.

Bresz, F. P. (2004). People often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance*, *6*(4), 57–60.

Broadhurst, R., & Chang, Y. (2012). Cybercrime in Asia:Trend and challenges. In *Asian Handbook of Criminology* (pp. 1–26).

Brown, P. C., Dunn, M. E., & Budney, A. J. (2014). Development and initial evaluation of a web-based program to increase parental awareness and monitoring of underage alcohol use: A brief report. *Journal of Child & Adolescent Substance Abuse*, *23*(2), 109–115.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548.

Busch, J. R., O'Brien, T. P., & Spangler, W. D. (2005). Increasing the quantity and quality of school leadership candidates through formation experiences. *Journal of Leadership and Organizational Studies*, *11*(3), 95–108.

Butler, M. M., Brosnan, M. C., Drennan, J., Feeney, P., Gavigan, O., Kington, M., … Walsh, M. C. (2014). Evaluating midwifery-led antenatal care: using a programme logic model to identify relevant outcomes. *Midwifery*, *30*(1), e34–e41.

Caetano, R. V. A. (2007). Training transfer: the mediating role of perception of learning. *Journal of European Industrial Training*, *31*(4), 283–296.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, *12*(1), 28–38.

Carmines, E. G., & Zeller, R. . (1979). *Reliability and validity assessment*. Sage Publications Inc.

Cass, A., Shaw, T., Ehman, M., Young, J., Flood, J., & Royce, S. (2013). Improved outcomes found after implementing a systematic evaluation and program improvement process for tuberculosis. *Public Health Reports*, *128*(5), 367–376. Retrieved from

Chang, Y.-H. E. (2010). *An empirical studt of Kirkpatrick's evaluation model in hospitality industry*. Florida International University.

Charoen, D., Raman, M., & Olfman, L. (2007). Improving end user behaviour in password utilization: An action research initiative. *Systemic Practice and Action Research*, *21*(1), 55–72.

Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). Online obscenity and child sexual abuse. In *Cybercrime, Digital Forensics and Jurisdiction* (pp. 81–94). Springer International Publishing.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness : A case study of an information security awareness system. *Information Technology, Learning and Performance Journal*, *24*(1), 1–15.

Chenwo, K. (2012). Evaluation of e-learning effectiveness in culture and arts promotion: The case of cultural division in Taiwan. *Journal of Information Technology and Application in Education*, *1*(1), 9–18.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731.

Christodoulaki, M., & Fragopoulou, P. (2010). SafeLine: reporting illegal internet content. *Information Management & Computer Security*, *18*(1), 54–65.

Christopherson, K. . (2006). The positive and negative implications of anonymity in Internet social interactions: ‘“on the Internet, nobody knows you”re a dog. *Computer in Human Behavior*, *23*(2007), 3038–3056.

Ciampa, M. (2013). *Security awareness: Applying practical security in your world*. Cengage Learning.

Clement, T., & Bigby, C. (2011). The development and utility of a program theory: Lessons from an evaluation of a reputed exemplary residential support service for adults with intellectual disability and severe challenging behaviour in Victoria, Australia. *Journal of Applied Research in Intellectual Disabilities*, *24*(6), 554–565.

Cole, J. I., Suman, M., Schramm, P., Zhou, L., & Salvador, A. (2013). The digital future report 2013 surveying the digital future year eleven. Retrieved July 2, 2014, from http://www.digitalcenter.org/wp-content/uploads/2013/06/2013-Report.pdf

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*(1), 63–72

.

Cooksy, L. J., Gill, P., & Kelly, P. A. (2001). The program logic model as an integrative framework for a multimethod evaluation. *Evaluation and Program Planning*, *24*(2), 119–128.

Cooper, D. R., Schindler, P. S., & Sun, J. (2003). *Business research method (12th ed)*. Pennsylvania State: McGraw-Hill Irwin.

Cornish, E. (1996). The cyber future: 92 ways our lives will change by the year 2025. *The Futurist*, *30*(1), SS1.

Correa, T., Straubhaar, J. D., Chen, W., & Spence, J. (2013). Brokering new technologies: The role of children in their parents' usage of the internet. *New Media & Society*, *1461444813*.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Creswell, J. (2009). *Research design: Qualitative, Quantitative, Mixed Method Approaches*. Sage publications.

Creswell, J. W., Clark, Plano L., V., Gutmann, M. L., & Hanson, W. E. (2003). *Advanced mixed methods research designs. Handbook of mixed methods in social and behavioral research*. Thousand Oaks, CA: Sage

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101.

Custers, B., Van der Hof, S., Schermer, B., & Appleby-Arnold, S. Brockdorff, N. (2013). Informed consent in social media use. The gap between user expectations and EU personal data protection law. *SCRIPTed Journal of Law, Technology and Society*, *10*(4), 435–457.

CyberSecurity Malaysia. (2012). *ESecurity buletin*. Retrieved from http://www.cybersecurity.my/data/content_files/12/1078.pdf

Da Veiga, A. (2015). An information security training and awareness approach (ISTAAP) to instil an information security-positive culture. In *Proceedings of the ninth international symposium on human aspects of information security and assurance (HAISA 2015)*.

Davis, F. D., & Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments. *International Journal of Human-Computer Studies*, *45*(1), 19–45.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, *35*(8), 982–1003.

De Moor, S., Dock, M., Gallez, S., Lenaerts, S., Scholler, C., & Vleugels, C. (2008). Teens and ICT: Risks and opportunities. Retrieved July, 16, 2015.

De Troyer, O., Van Broeckhoven, F., & Vlieghe, J. (2017). Linking serious game narratives with pedagogical theories and pedagogical design strategies. *Journal of Computing in Higher Education*, 1–25.

DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research*, *3*(1), 60–95.

DiVall, M., Barr, J., Gonyeau, M., Matthews, S. J., Van Amburgh, J., Qualters, D., & Trujillo, J. (2012). Follow-up assessment of a faculty peer observation and evaluation program. *American Journal of Pharmaceutical Education*, *76*(4), 61

.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*(3–4), 189–198.

Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). Measuring a Cybersecurity Program. In *Enterprise Cybersecurity* (pp. 213–229). Apress.

Donaldson, S. I. (2012). *Program theory-driven evaluation science: Strategies and applications*. Routledge.

Drevin, L., Kruger, H. a., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security*, *26*(1), 36–43.

Fahrnberger, G. (2014). A comprehensive approach for a secure instant messaging sifter. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 164–173).

Farjad, S. (2012). The evaluation effectiveness of training courses in university by Kirkpatrick model (case study: Islamshahr university). *Procedia - Social and Behavioral Sciences*, *46*, 2837 – 2841.

Farmer, J., & Reupert, A. (2013). Understanding autism and understanding my child with autism: an evaluation of a group parent education program in rural Australia. *The Australian Journal of Rural Health*, *21*(1), 20–7.

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. In *2015 IEEE Trustcom/BigDataSE/ISPA* (pp. 352–359). IEEE.

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials*, *16*(4), 2019–2036.

Fitton, V. A., Ahmedani, B. K., Harold, R. D., & Shifflet, E. D. (2013). The role of technology on young adolescent development: Implications for policy, research and practice. *Child and Adolescent Social Work Journal*, *30*(5), 399–341.

Fitzpatrick, J. L., Sanders, J. R., & Worthen, B. R. (2004). *Program evaluation: Alternative approaches and practical guidelines*. Retrieved July 29 2014. http://dissertation.argosy.edu/chicago/spring08/r7036_sp08nowlin.doc

Fitzpatrick, J. L., Sanders, J. R., & Worthen, B. R. (2012). Program-oriented evaluation approaches. In *Program Evaluation Alternative Approaches and Practical Guideline* (Fourth, pp. 161–164). Pearson Education Inc.

Frye, A. W., & Hemmer, P. a. (2012). Program evaluation models and related theories: AMEE guide no. 67. *Medical Teacher*, *34*(5), e288–e299.

Furman, S., Theofanos, M. F., Choong, Y. Y., & Stanton, B. (2012). Basing cybersecurity training on user perceptions. *IEEE Security and Privacy*, *10*(2), 40–49.

Furnell, S. (2008). End-user security culture : A lesson that will never be learnt? *Computer Fraud & Security*, (April), 6–9.

Furnell, S. (2010). Jumping security hurdles. *Computer Fraud & Security*, *2010*(6), 10–14. https://doi.org/10.1016/S1361-3723(10)70067-1

Furnell, S. M., Bryant, P., & Phippen, A. . (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410–417. https://doi.org/10.1016/j.cose.2007.03.001

Furnell, S., & Thomson, K.-L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security*, *2009*(2), 5–10. https://doi.org/10.1016/S1361-3723(09)70019-3

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & Security*, *27*(7–8), 235–240. https://doi.org/10.1016/j.cose.2008.01.001

Galliers, R. D., & Huang, J. C. (2011). The teaching of qualitative research methods in information systems: an explorative study utilizing learning theory. *European Journal of Information Systems*, *21*(2), 119–134. https://doi.org/10.1057/ejis.2011.44

Gibbs, A. (1997). Focus groups. *Social Research Update*, *19*(8), 1–8.

Goverment of Malaysia. Personal Data Protection Act 2010 (2010). Malaysia. Retrieved from http://www.kkmm.gov.my/pdf/Personal Data Protection Act 2010.pdf

Goverment of United Kingdom. United Kingdom Data Protection Act 1998 (1998). United Kingdom. Retrieved from http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf

Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. *Educational Evaluation and Policy Analysis*, *11*(3), 255–274.

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quaterly*, *30*(3), 611–642. Retrieved from http://www.jstor.org/stable/25148742

Gross, J. B., & Rosson, M. B. (2007). Looking for trouble. In *Proceedings of the 2007 symposium on Computer human interaction for the management of information technology - CHIMIT '07* (p. 10). New York, New York, USA: ACM Press. https://doi.org/10.1145/1234772.1234786

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *WPES '05 Proceedings of the 2005 ACM WORKSHOP on Privacy in the electronic society* (pp. 71–80). https://doi.org/1-59593-228-3/05/0011

Grzeskowiak, L. E., Alicia E. Thomas, Alicia E. To, J., Phillips, A. J., & Reeve, E. (2015). Enhancing education activities for health care trainees and professionals using audience response systems: A systematic review. *Journal of Continuing Education in the Health Professions*, *35*(4), 261–269.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Gupta, S., & Kumaraguru, P. (2014). Emerging phishing trends and effectiveness of the anti-phishing landing page. In APWG Symposium (Ed.), *Electronic Crime Research (eCrime)* (pp. 36–47). IEEE.

Hagen, J., Albrechtsen, E., & Ole Johnsen, S. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security*, *19*(3), 140–154.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152.

Halal, W. E., & Liebowitz, J. (1994). Telelearning: The multimedia revolution in education. *The Futurist*, *28*(6), 21.

Hansen, A., Cottlr, S., Negrine, R., & Newbold, C. (1998). *Mass communication research methods*. Palgrave Macmillan.

Haynes, S. N., Richard, D., & Kubany, E. S. (1995). Content validity in psychological assessment: A functional approach to concepts and methods. *Psychological Assessment*, *7*(3), 238.

Helbing, D. (2015). Big data, privacy, and trusted web: What needs to be done. In *Thinking Ahead-Essays on Big Data, Digital Revolution, and Participatory Market Society* (pp. 115–176). Springer International Publishing.

Higgins, A., Sharek, D., Nolan, M., Sheerin, B., Flanagan, P., Slaicuinaite, S., Walsh, H. (2012). Mixed methods evaluation of an interdisciplinary sexuality education programme for staff working with people who have an acquired physical disability. *Journal of Advanced Nursing*, *68*(11), 2559–2569. https://doi.org/10.1111/j.1365-2648.2012.05959.x

Ho, R. (2014). *Second Edition: Handbook of Univariate and Multivariate Data Analysis eith IBM SPSS*. CRC press

Ho, W.-W., Chen, W.-J., Ho, C.-K., Lee, M.-B., Chen, C.-C., & Chou, F. H.-C. (2011). Evaluation of the suicide prevention program in Kaohsiung City, Taiwan, using the CIPP evaluation model. *Community Mental Health Journal*, *47*(5), 542–550. https://doi.org/10.1007/s10597-010-9364-7

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: an integrated conceptualization and four empirical studies. *MIS Quaterly*, *37*(1), 275–298.

Ilesanmi, A. O. (2010). Post-occupancy evaluation and residents' satisfaction with public housing in Lagos, Nigeria. *Journal of Building Appraisal*, *6*(2), 153–169. https://doi.org/10.1057/jba.2010.20

ITU. (2014). The world in 2014: ICT facts and figures. Retrieved April 29, 2015, from www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

Joe, M. M., & Ramakrishnan, D. B. (2014). A survey of various security issues in online social networks. *International Journal of Computer Networks and Applications*, *1*(1), 11–14.

Johansson, A., & Götestam, K. G. (2004). Internet addiction: characteristics of a questionnaire and prevalence in Norwegian youth (12-18 years). *Scandinavian Journal of Psychology*, *45*(3), 223–229. https://doi.org/10.1111/j.1467-9450.2004.00398.x

Johnson, E. C. (2006). Security awareness : Switch to a better programme. *Network Security*, (February), 15–18.

Johnson, J., Hall, J., Greene, J. C., & Ahn, J. (2013). Exploring alternative approaches for presenting evaluation results. *American Journal of Evaluation*, *34*(4), 486–503. https://doi.org/10.1177/1098214013492995

Johnson, R. B., & Onwuegbuzie, A. J. (2004a). Mixed method research: A research paradigm whose time has come. *Educational Researcher*, *33*(7), 14–26.

Johnson, R. B., & Onwuegbuzie, A. J. (2004b). Mixed method research: A research whose time has come. *Educational Researcher*, *33*(7), 14–26.

Kaplan, A. M., & Haenlein, M. (2010). (2010). Users of the world, unite! the challenges and opportunities of social media. *Business Horizons*, *53*(1), 59–68.

Kaye, J. 'Jofish'. (2011). Self-reported password sharing strategies. In *CHI 2011 • Session: Authentication* (pp. 2619–2622).

Keay, L., Hunter, K., Brown, J., Simpson, J. M., Bilston, L. E., Elliott, M., … Ivers, R. Q. (2012). Evaluation of an education, restraint distribution, and fitting program to promote correct use of age-appropriate child restraints for children aged 3 to 5 years: A cluster randomized trial. *American Journal of Public Health*, *102*(12), e96–e102. https://doi.org/10.2105/AJPH.2012.301030

Keller, J. M., & Kopp, T. W. (1987). An application of the ARCS Model of Motivational Design. In *Instructional theories in action: Lessons illustrating selected theories and models* (pp. 289–320). Hillsdale, NJ, US: Lawrence Erlbaum Associates, Inc.

Kirkpatrick, D. (1994). *Evaluating training programs: four levels*. San Francisco, CA, US: Berrett-Koehler.

Kirkpatrick, D. L. (2009). *Implementing the four levels: A practical guide for effective evaluation of training programs* (Easyread S). ReadHowYouWant. com.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, 67–93.

Kleina, E. ., Tellefsenb, T., & Herskovitzc, P. . (2007). The use of group support systems in focus groups: Information technology meets qualitative research. *Computer in Human Behavior*, *23*(5), 2113–2132.

Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice*, *13*(5), 66.

Kok, E. T., Ng, M. L. Y., & Kim, G. S. (2010). Online activities and writing practices of urban Malaysian adolescents. *System*, *38*(4), 548–559. https://doi.org/10.1016/j.system.2010.09.014

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840–847.

Kruger, H., Drevin, L., & Steyn, T. (2006). A framework for evaluating ICT security awareness. In *ISSA* (pp. 1–11). Retrieved from icsa.cs.up.ac.za

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, *18*(5), 316–327. https://doi.org/10.1108/09685221011095236

Kruger, H., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Labuschagne, W. A., Burke, I., Veerasamy, N., & Eloff, M. M. (2011). Design of cyber security awareness game utilizing a social media framework. In *Information Security for South Africa* (pp. 1–9). IEEE.

Lai, W. F., & Ngerng, M. H. (2015). Analysis of Decision Making on Selection of the Social Networking Sites by College Students. *Pertanika Journal of Social Sciences & Humanities*, *23*.

Lanier, J. (2013). Privacy?, How Should We Think about. *Scientific American*, *309*(5), 64–71.

LaRose, R., Lin, C. A., & Eastin, M. S. (2003). Unregulated Internet usage: Addiction, habit, or deficient self-regulation? *Media Psychology*, *5*(3), 225–253.

Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation*. Cambridge university press.

Laven, D., Ventriss, C., Manning, R., & Mitchell, N. (2010). Evaluating U.S. national heritage areas: Theory, methods, and application. *Environmental Management*, *46*(2), 195–212. https://doi.org/10.1007/s00267-010-9514-2

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, *22*(8), 285–292.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., … Wolff, S. S. (1997). The past and future history of the Internet. *Communications of the ACM*, *40*(2), 102–108.

Lenhart, A. (2012). *Teens, smartphones & texting*. Pew Internet & American Life Project, 1-34.

Lenhart, A. (2015). *Teens, social media & technology overview 2015*. Pew Internet & American Life Project.

Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickhur, K., & Rainie, L. (2011). *Teens, kindness and cruelty on social network sites*. Pew Internet & American Life Project.

Lenhart, A., Purcell, K., Smith, A., & Zickhur, K. (2010). *Social media and mobile internet use among teens and youngs adults*. Pew Internet and American Life Project.

Lewis, J. A. (2014). Cyber threat and response combating advanced attacks and cyber espionage. *Centre for Strategic & International Studies*, 1–8.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry (Vol. 75). Sage Publications Inc.

Lincoln, Y. S., & Guba, E. G. (2000). *Paradigmatic controversies, contradictions and emerging confluences* (Y.S. Linco). Thousand Oaks, CA: Sage.

Livingstone, S., Bober, M., & Helsper, E. (2005). *Internet literacy among children and young people : findings from the UK children go online project Internet literacy among children and young people*. OFCOM/ESRC, London, UK.

Loibl, T. R. (2005). Identity theft, spyware and the law. In *InfoSecCD Conference* (pp. 118–121).

Louw, J. (2012). Programme evaluation: Can it improve human resource management practice? *SA Journal of Human Resource Management*, *10*(3). https://doi.org/10.4102/sajhrm.v10i3.428

Lucero, J. ., Weisz, A. ., Smith-Darden, J., & Lucero, S. . (2014). Exploring gender differences: Socially interactive technology use/abuse among dating teens. *Journal of Women and Social Work*, *29*(4), 478–491. https://doi.org/10.1177/0886109914522627

Mackenzie, N., & Knipe, S. (2006). Research dilemmas: Paradigms, methods and methodology. *Issues in Educational Research*, *16.2*, 193–205.

Madaus, G. F., Scriven, M., Stufflebeam, & (Eds.)., D. L. (2012). *Evaluation models: Viewpoints on educational and human services evaluation Vol 6*. Springer Science & Business Media.

Madden, M., Lenhart, A., Duggan, M., Cortesi, S., & Grasser, U. (2013). *Teen and technology 2013*. Pew Internet & American Life Project.

Malaysian Communication and Multimedia Commision. (2013). *Internet users survey 2012*. Retrieved from http://www.skmm.gov.my/skmmgovmy/media/General/pdf/InternetUsersSurvey2012.pdf

Malaysian Communication and Multimedia Commision. (2014). *Internet users survey 2014*. Retrieved from http://www.mcmc.gov.my/

Manap, N. A. (2013). The influence of E-ASEAN in the development of ICT Law in Malaysia. *International Journal of Soft Computing*, *8*(5), 377–380.

Manap, N. A., Basir, S. M., Hussein, S. M., Tehrani, P. M., & Rouhani, A. (2013). Legal issues of data protection in cloud computing. *International Journal of Soft Computing*, *8*(5), 371–376.

Mani, D., Choo, R., & Mubarak, S. (2014). Information security in the South Australian real estate industry: A study of 40 real estate organisations. *Information Management & Computer Security*, *22*(1), 24–41.

May, C. (2008). Approaches to user education. *Network Security*, (September).

Mazurek, M. L., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., & B, U. (2013). Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 173–186).

McClelland, J. L., Rumelhart, D. E., & P. R. G. (1987). Parallel distributed processing. In *Parallel distributed processing Vol 2*. Cambridge, MA: MIT Press.

Meekin, S. (2016). 2016 Blamey Oration: The cyber and space domains in 21st century warfare. *United Service*, *67*(3), 9.

Mertens, D. M., & Wilson, A. T. (2012a). *Program evaluation theory and practice* (1st ed.). New York: The Guilford Press.

Mertens, D. M., & Wilson, A. T. (2012b). *Program evaluation theory and practice: A comprehensive guide*. Guilford Press.

Mertens, D.M (2005). *Research methods in education and psychology: Integrating diversity with quantitative and qualitative approaches (2nd ed.)*. Thousand Oaks: Sage.

Mertens, D. M. (1998). *Research methods in education and psychology: Integrating diversity with quantitative and qualitative approaches*. Thousand Oaks, CA: Sage.

Mertens, D. M. (2014). *Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods*. Sage Publications Inc.

Meter, D. J., & Bauman, S. (2015). When sharing is a bad idea: the effects of online social network engagement and sharing passwords with friends on cyberbullying involvement. *Cyberpsychology, Behavior, and Social Networking*, *18*(8), 437–442.

Mhlaba, S. L. (1995). Who Determines What Our Children See, Read, Do, or Learn on the Internet? *Trotter Review*, *9*(2), 4.

Micheli, M. (2015). What is new in the digital divide? Understanding internet use by teenagers from different social backgrounds. *Communication and Information Technologies Annual.*, *Digital di*, 55–87.

Miller, G. A. (1956). The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological Review*, *63*(2), 81.

Mingers, J., & Brocklesby, J. (1997). Multimethodology: for mixing towards a framework methodologies. *International Journal Management Science*, *25*(5), 489–509.

Morrow, V., & Richards, M. (1996). The ethics of social research with children: An overview1. *Children & Society*, *10*(2), 90–105.

Morton, A. (2014). "Age shall not wither them": but it will change their priorities about protecting their information privacy. In *2014 ASE BigData/SocialInformatics/PASSAT/BioMedCom 2014 Conference*. Harvard University.

Mugenda, O. M. (1999). Research methods: Quantitative and qualitative approaches. *African Centre for Technology Studies*.

Nabukenya, J., Van Bommel, P., Proper, H. A., & De Vreede, G.-J. (2009). An evaluation instrument for collaborative processes: Application to organizational policy-making. *Group Decision and Negotiation*, *20*(4), 465–488. https://doi.org/10.1007/s10726-009-9177-7

Neuman, L. W. (2002). *Social research methods: Qualitative and quantitative approaches (5th Edition)*.

Newcomer, K. E., Hatry, H. P., & Wholey, J. S. (2015). *Handbook of practical program evaluation*. John Wiley & Sons.

Newman, G. R., & Mcnally, M. M. (2005). *Identity theft literature review*. U.S. Department of Justice

Newman, R. C. (2006). Cybercrime, identity theft , and fraud : Practicing safe Internet - network security threats and vulnerabilities. In *Proceedings of the 3rd annual conference on Information security curriculum development - InfoSecCD '06*.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

O'Keeffe, G. S., Clarke-Pearson, K., & Council on Communications and Media. (2011). The impact of social media on children, adolescents, and families. *Pediatrics*, *127*(4), 800–804. https://doi.org/10.1542/peds.2011-0054

Oblinger, D., & Oblinger, J. (2005). Is it age or IT: First steps toward understanding the net generation. *Educating the Net Generation*, *2*(1–2), 20.

Odoemelam, C. E. (2015). Adapting to surveillance and privacy issues in the era of technological and social networking. *International Journal of Social Science and Humanity*, *5*(6), 572.

Ólafsson.K, S, L., & L, H. (2013). *How to research children and online technologies? Frequently asked questions and best practice*

Osma Ruiz, V. J., Saenz Lechón, N., Gutiérrez Arriola, J. M., Argüelles Álvarez, I., Fraile Muñoz, R., & Marcano Ganzo, R. (2015). Learning English is fun! Increasing motivation through video games. In *ICERI2015 Proceedings* (pp. 6307–6316). Sevilla.

Park, S., Na, E. Y., & Kim, E. M. (2014). The relationship between online activities, netiquette and cyberbullying. *Children and Youth Services Review*, *42*, 74–81.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117–129.

Pather, S., & Remenyi, D. (2004). Some of the philosophical issues underpinning research in information systems: from positivism to critical realism. In *Proceedings of the 2004 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* (pp. 141–146). South African Institute for Computer Scientists and Information Technologists.

Patton, M. Q. (1990). *Qualitative evaluation and research methods*. Sage Publications Inc.

Peltier, T. R. (2005). Implementing an information security awareness program. *Information Systems Security*, *14*(2), 37–49. https://doi.org/10.1201/1086/45241.14.2.20050501/88292.6

Pogrund, R. L., Darst, S., & Boland, T. (2013). Evaluation study of short-term programs at a residential school for students who are blind and visually impaired. *Journal of Visual Impairment & Blindness*, (January-February), 30–42.

Power, E. M. (2007). Developing a culture of privacy: A case study. *IEEE Security & Privacy Magazine*, 58–60.

Pramod, D., & Raman, R. (2014). A study on the user perception and awareness of smartphone security. *A Study on the User Perception and Awareness of Smartphone Security*, 0973–4562.

Praslova, L. (2010). Adaptation of Kirkpatrick's four level model of training criteria to assessment of learning outcomes and program evaluation in Higher Education. *Educational Assessment, Evaluation and Accountability*, *22*(3), 215–225.

Rafiq, M. (2015). Training evaluation in an organization using Kirkpatrick model: A case study of PIA. *Entrepreneurship & Organization Management*, *4*(3), 151.

Rahim, N. H. A., Hamid, S., Mat Kiah, M. L. Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), 606–622.

Ramli, N. S., Hassan, M., Osman, M. N., Shaffril, M., & Azril, H. (2014). Qualitative findings on youths views on the internet and mobile phone: the case of university students in Malaysia. *The Social Sciences*, *9*(3), 239–243.

Rani, P., & Shukla, S. C. (2012). Learning style in education. *International Journal of Research in Economics & Social Sciences*, *2*(5).

Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How effective is your security awareness program? An evaluation methodology. *Information Security Journal: A Global Perspective*, *21*(6), 328–345. https://doi.org/10.1080/19393555.2012.747234

Reid, D. J., & Reid, F. J. . (2005). Online focus groups An in-depth comparison of computermediated and conventional focus group discussions. *International Journal of Market Research*, *47*(2), 131–162.

Reynolds, H. W., & Sutherland, E. G. (2013). A systematic approach to the planning, implementation, monitoring, and evaluation of integrated health services. *BMC Health Services Research*, *13*(168), 1–11. https://doi.org/10.1186/1472-6963-13-168

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7–8), 241–253. https://doi.org/10.1016/j.cose.2008.07.008

Richet, J. L. (2015). How to become a cybercriminal? *Human Behavior, Psychology, and Social Interaction in the Digital Era*, *229*.

Robbins, L. B., Pfeiffer, K. A., Wesolek, S. M., & Lo, Y.-J. (2014). Process evaluation for a school-based physical activity intervention for 6th- and 7th-grade boys: Reach, dose, and fidelity. *Evaluation and Program Planning*, *42*, 21–31. https://doi.org/10.1016/j.evalprogplan.2013.09.002

Rogers, P. J., Petrosino, A., Huebner, T. A., & Hacsi., T. A. (2000). Program theory evaluation: Practice, promise, and problems. *New Directions for Evaluation*, *2000*(87), 5–13.

Rossi, P. H., Lipsey, M. W., & Freeman, H. E. . (2004). *Evaluation: A systematic approach*. USA: Sage Publications Inc.

Royse, D., & Thyer, B. A. Padgett, D. K. (2015). *Program evaluation: An introduction to an evidence-based approach*. Cengage Learning.

Royse, D., Thyer, B. A., Padgett, D. K., & Logan, T. K. (2001). *Program evaluation an introduction*. Cengage Learning.

Saran, S. (2016). Striving for an International Consensus on Cyber Security: Lessons from the 20th Century. *Global Policy*, *7*(1), 93–95.

Schall, Patricia L., & Skeele, R. (1995). Creating a homeschool partnership for learning: Exploiting the home computer. *Educational Forum*, *59*(3), 244–249.

Scriven, M. (1967). *The methodology of evaluation*. Chicago: Rand McNally.

Shadish, W. R., Cook, T. D., & Leviton, L. C. (1991). *Foundations of program evaluation: Theories of practice*. Sage Publications Inc.

Shadish, W. R. (1998). Evaluation theory is who we are. *American Journal of Evaluation*, *19*(1), 1–19.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Shenton, A. K., & Dixon, P. (2004). Issues arising from youngsters' information-seeking behavior. *Library & Information Science Research*, *26*(2), 177–200.

Shin, W., & Kang, H. (2016). Adolescents' privacy concerns and information disclosure online: the role of parents and the Internet. *Computers in Human Behavior*, *54*, 114–123.

Sieber, S., & Sabatie, J. V. (2003). Uses and attitudes of young people toward technology and mobile telephony. In *16th Bled eCommerce Conference eTransformation* (pp. 773–787). Bled, Slovenia.

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., & Furlong, M. (2007). Password sharing: implications for security design based on social practice. In *In Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 895–904).

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(Table I), 31–41.

Sithira, V., & Nguwi, Y. (2014). A study on the adolescent online security issues. *International Journal of Multidisciplinary and Current Research*, *2*(June), 596–601.

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, *8*(4), 3–26.

Smahel, D., Helsper, E., Green, L., Kalmus, V., Blinka, L., & Ólafsson, K. (2012). *Excessive internet use among European children*.

Soffer, T., & Cohen, A. (2015). Privacy perception of adolescents in a digital world. *Bulletin of Science, Technology & Society*, *270467615*.

Somekh, B., & Lewin, C. (2005). *Research methods in the social sciences*. Thousand Oaks: Sage.

Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K. L. (2015). The challenges of personal data markets and privacy. *Electronic Markets*, *25*(2), 161–167.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Steinberg, L., & Cauffman, E. (1996). Maturity of judgment in adolescence: Psychosocial factors in adolescent decision making. *Law and Human Behavior*, *20*(3), 249.

Stolzenberg, R. M. (2004). *Multiple regression analysis. Handbook of data analysis*. England: Sage London.

Stufflebeam, D. L., & Shinkfield, A. J. (2007). *Evaluation theory, models, and applications*. John Wiley & Sons.

Suraya, H. (2013). *The use of online social networking (OSN) for higher education*. The University of Melbourne Australia.

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. In *2010 International Conference on Availability, Reliability and Security* (pp. 196–203). Ieee. https://doi.org/10.1109/ARES.2010.27

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: A tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233–244. https://doi.org/10.1080/01449290903121386

Tan, K., & Newman, E. (2013). The evaluation of sales force training in retail organizations: A test of Kirkpatrick's four-level model. *International Journal of Management*, *30*(2), 692–703.

Tashakkori, A., & Teddlie, C. (2003). *Handbook of mixed methods in social and behavioural research*. London: Cassell.

Tene, O., & Polonetsky, J. (2012). Privacy in the age of big data: a time for big decisions. *Stanford Law Review Online*, *64*, 63.

Thomson, M. E., & Solms, R. von. (1998). Information security awareness : educating your users effectively. *Information Management & Computer Security*, *5*(4), 167–173.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2014). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*(1), 38–58.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal: A Global Perspective*, *17*(5–6), 207–227. https://doi.org/10.1080/19393550802492487

Turner III, D. W. (2010). Qualitative interview design: A practical guide for novice investigators. *The Qualitative Report*, *15*(3), 754.

Valcke, M., De Wever, B., Van Keer, H., & Schellens, T. (2011). Long-term study of safe Internet use of young children. *Computers & Education*, *57*(1), 1292–1305.

Valentine, J. A., & Labs, I. (2006). Enhancing the employee security awareness model. *Computer Fraud & Security*, *2006*(6), 17–19.

van den Eertwegh, V., van Dulmen, S., van Dalen, J., Scherpbier, A. J. J. A., & van der Vleuten, C. P. M. (2013). Learning in context: Identifying gaps in research on the transfer of medical communication skills to the clinical workplace. *Patient Education and Counseling*, *90*(2013), 184–192.

Vandoninck, S., D'Haenens, L., & Smahel, D. (2014). *Preventive measures – how youngsters avoid online risks*. Retrieved from www.eukidsonline.net

Vedder, A., & Wachbroit, R. (2003). Reliability of information on the Internet: Some distinctions. *Ethics and Information Technology*, *5*(4), 211–215.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quaterly*, 425–478.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bringing the qualitative -quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quaterly*, *37*(1), 21–54.

Vogel, T., & Wanke, M. (2016). *Attitudes and attitude change*. Psychology Press.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wainer, H., & Braun, H. I. (2013). *Test validity*. Routledge.

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2015). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *6*(1). https://doi.org/http://dx.doi.org/10.5817/CP2012-1-3

Warren, P., & Streeter, M. (2013). *Cyber crime & warfare: All that matters.* UK: Hachette.

Weinstein, E. C., & Selman, R. L. (2014). Digital stress: Adolescents' personal accounts. *New Media & Society*, *1461444814*.

WenJie, W., Yufei, Y., & Archer, N. (2006, March). A contextual framework for combating identity theft. *IEEE Security & Privacy Magazine*, *4*(2), 30–38. https://doi.org/10.1109/MSP.2006.31

Whitson, J. (2009). Identity theft and the challenges of caring for your virtual self. *Interactions*, *16*(2), 41. https://doi.org/10.1145/1487632.1487642

Willingham, W. W., & Cole, N. S. (2013). Gender and fair assessment. Routledge.

Willard, N. (2006). *Cyberbullying and cyberthreats*. Center for Safe and Responsible Internet Use.

Yampolskaya, S., Nesman, T. M., Hernandez, M., & Koch, D. (2004). Using concept mapping to develop a logic model and articulate a program theory: A case example. *American Journal of Evaluation*, *25*(2), 191–207.

Yarbrough, D. B., Shulha, L. M., Hopson, R. K., & Caruthers, F. A. (2011). *The program evaluation standards: A guide for evalators and evaluation users*. California: Sage Publications, Inc.

Yardley, S., & Dornan, T. (2012). Kirkpatrick's levels and education "evidence." *Medical Education*, *46*, 97–106.

Yeh, Y.-T., Chen, H.-Y., Cheng, K.-J., Hou, S.-A., Yen, Y.-H., & Liu, C.-T. (2014). Evaluating an online pharmaceutical education system for pharmacy interns in critical care settings. *Computer Methods and Programs in Biomedicine*, *113*(2), 682–689. https://doi.org/10.1016/j.cmpb.2013.11.006

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *The Journal of Consumer Affairs*, *43*(3), 389–418.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, *16*(4), 479–500.