THE EFFECTS OF STRUCTURED VERSUS UNSTRUCTURED ONLINE TRAINING MODULES ON CYBER SECURITY AWARENESS AND PERCEIVED BEHAVIOUR AMONG COLLEGE STUDENTS

LALITHA MUNIANDY

UNIVERSITI SAINS MALAYSIA

2017

THE EFFECTS OF STRUCTURED VERSUS UNSTRUCTURED ONLINE TRAINING MODULES ON CYBER SECURITY AWARENESS AND PERCEIVED BEHAVIOUR AMONG COLLEGE STUDENTS

by

LALITHA MUNIANDY

Thesis submitted in fulfillment of the requirements
for the degree of
Doctor of Philosophy

November 2017

ACKNOWLEDGEMENT

I would like to thank all the people who contributed in some way to the work described in this thesis. First and foremost, I would like to express my special appreciation and thanks to my supervisor, Professor Dr. Balakrishnan Muniandy. Professor, you have been a tremendous mentor for me. I would like to thank you for encouraging my research and for allowing me to grow as a research scientist. Your advice on both research as well as on my career have been priceless. I would also like to thank my co-supervisor, Assoc. Professor Dr Zarina Samsudin. You have been very supportive throughout this journey. My sincere appreciation to both of you, who were always there for me. Thanks again for all your brilliant comments and suggestions. I wouldn’t be here without both of you.

Special thanks goes to MyBrain15 which have provided financial assistance to complete my studies. Further, I also would like to thank all academic staff and administrative staff in CiTM. My special thanks to Professor Dr Irfan Naufal Umar, Assoc. Professor Wan Ahmad Jaafar Wan Yahaya, Dr Mariam Mohamad and Assoc. Professor Dr Mona Masood. All your useful feedback and insightful comments on my work, which I received during my proposal defend greatly help me to improve my PhD thesis. Thank you very much.

I also would like to convey my gratitude to all the respondents who had participated in my study. I also would like to thank the management of Tunku Abdul Rahman University College, who allowed me to further my studies as well as permitted me to conduct my study in their site. My special gratitude to all the subject matter experts who had validated my instruments and my online training modules. Thank you Dr

Kang Seok Hoon, Assoc. Professor Dr Janice Toh Guat Guan, Professor Steven Furnell, Dr Fariza Hanis Abdul Razak, Ms Karamjeet Kaur, Dr Subashini Annamalai for your great support and useful feedback.

A very special and sincere thanks to my family. Words cannot express how grateful I am to my beloved husband, Mr Gunasegaran and two most wonderful yet very understanding daughters, Soumiyaa and Thanushiya. Thank you for all the sacrifices that you've made on my behalf. Thank you for all your love and support. I sincerely appreciate all your sacrifices and support. My greatest appreciation to my parents, Mr Muniandy and Madam Seetha Letchimi, as well as my in-laws, Mr Albib , Madam Ambiga and Madam Thaivayanai. Your prayers for me was what sustained me this far and to strive towards my goal. Finally, I would like to thank my siblings, Madam Puspa Mala, Madam Eswari and Mr Sivaraj and their families, who were very supportive and helpful throughout this journey.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

CHAPTER 2: LITERATURE REVIEW

CHAPTER 3: RESEARCH METHODOLOGY

CHAPTER 4: DESIGN AND DEVELOPMENT

CHAPTER 5: DATA ANALYSIS

LIST OF TABLES

LIST OF FIGURES

KESAN MODUL LATIHAN ATAS TALIAN BERSTRUKTUR DAN TIDAK BERSTRUKTUR KE ATAS KESEDARAN DAN PERSEPSI TINGKAH LAKU KESELAMATAN SIBER PELAJAR KOLEJ

ABSTRAK

Kajian ini menyiasat tentang kesan modul latihan atas talian berstruktur berbanding tidak berstruktur terhadap kesedaran dan persepsi tingkah laku keselamatan siber para pelajar kolej. Kedua-dua modul latihan atas talian ini merangkumi lima aspek keselamatan siber, iaitu penggunaan kata laluan, pancing, kejuruteraan sosial, penipuan atas talian dan perisian perosak. Kajian ini dijalankan di sebuah kolej universiti terkenal yang terletak di sebuah negeri di utara Semenanjung Malaysia. Seramai 240 orang responden dari empat fakulti dari kolej universiti terlibat dalam kajian ini. Rekabentuk kajian yang digunakan ialah reka bentuk separa eksperimen ujian pasca. Jenis motivasi (intrinsik dan ekstrinsik) serta bidang pengkhususan (teknikal dan bukan teknikal) para pelajar dimanipulasi sebagai faktor moderator. Terdapat dua jenis instrumen, *Intrinsic and Extrinsic Motivation Scale Questionnaire* (IEMSQ) dan *Cyber Security Behaviour and Awareness Instrument* (CSBAI) digunakan dalam kajian ini. IEMSQ digunakan untuk mengkategorikan responden mengikut jenis motivasi. CSBAI pula digunakan untuk mengkaji tahap kesedaran dan persepsi tingkah laku keselamatan siber responden selepas mereka mempelajari salah satu modul atas talian. Kedua-dua modul atas talian ini direka bentuk dengan mengunakan model instruksi ADDIE, Sembilan Peristiwa Pengajaran Gagne dan Teori Kognetif Pembelajaran Multimedia Mayer. Kandungan modul ini dihasilkan dengan mengaplikasikan *Protection Motivation Theory* (PMT). Dalam modul atas talian berstruktur, para responden telah mempelajari kandungan modul mengikut aliran yang telah ditetapkan. Dalam modul atas talian bukan berstruktur pula, para responden diberi pilihan untuk memilih dan belajar mana-mana sub modul kesukaan mereka. Dalam kajian ini, sebanyak enam hipotesis nul telah digubal. Kaedah analisis statistik inferens, ujian t kumpulan tidak bersandar dan ANOVA dua arah telah digunakan untuk menganalisis data. Keputusan kajian menunjukkan bahawa modul atas talian berstruktur adalah lebih berkesan daripada modul atas talian tidak berstruktur dalam memperbaiki persepsi kelakuan keselamatan siber. Namun, kedua-dua jenis modul berkesan dalam memupuk kesedaran keselamatan siber dalam kalangan para responden. Motivasi tidak menunjukkan kesan yang dijangkakan ke atas kesedaran atau persepsi tingkah laku keselamatan siber. Namun begitu, bidang pengkhususan para pelajar memainkan peranan yang penting dalam memupuk kesedaran keselamatan siber. Jenis modul atas talian memainkan peranan yang lebih penting berbanding bidang pengkhususan dalam mengubah persepsi tingkah laku keselamatan siber para pelajar. Kesimpulannya, pengajaran dan latihan amat penting dalam memupuk kesedaran keselamatan siber dan kelakuan keselamatan siber para pelajar kolej.

THE EFFECTS OF STRUCTURED VERSUS UNSTRUCTURED ONLINE TRAINING MODULES ON CYBER SECURITY AWARENESS AND PERCEIVED BEHAVIOUR AMONG COLLEGE STUDENTS

ABSTRACT

This study investigated the effects of structured versus unstructured online training module on college students' cyber security awareness and perceived cyber security behaviour. The two modes of online training modules were incorporated with the following cyber security aspects: password usage, phishing, social engineering, online scam and malware. The study was conducted in a well-established university college located in the Northern region of Peninsular Malaysia. A total of 240 respondents from four faculties of the university college participated in the study. A quasi-experimental, post-test design was adopted as a research design for the study. The respondents' motivation types (intrinsic and extrinsic) as well as specialization areas (technical and non-technical) were manipulated as the moderating factors. Two instruments, Intrinsic and Extrinsic Motivation Scale Questionnaire (IEMSQ) and Cyber Security Behaviour and Awareness Instrument (CSBAI) were used in this study. IEMSQ was used to categorize the respondents according to their motivation types. CSBAI was used to measure the cyber security awareness and perceived cyber security behaviour after the training. The two online training modules were designed using the ADDIE Model, Gagne's Nine Events of Instruction and Mayer's Cognitive Theory of Multimedia Learning. The contents of the modules were designed by incorporating Protection Motivation Theory (PMT). In structured online training module, the students were presented with the topics in a linear approach. The students were presented with the learning materials in predetermined sequence. Conversely, in unstructured online training module, the student could choose and learn the sub topics of the main module according to their preference. Six null hypotheses were formulated for this study. Inferential statistical analysis methods, independent groups *t*-test and two-way ANOVA were used to analyze the data. The results of the study showed that structured online training module is more effective than the unstructured online training module in changing the perceived cyber security behaviour of the respondents. Both modules effectively instilled cyber security awareness among the respondents. The effect of motivation type is limited while specialization area did influence the cyber security awareness of the respondents. The types of online training modules played a more important role than the specialization areas in improving the perceived cyber security behaviour of the respondents. This shows that education and training are important in addressing issues related to cyber security awareness and behaviour of college students.

CHAPTER 1

INTRODUCTION

1.1 Overview

The invention of the Internet and its related technologies had drastically changed the lives of its users. Internet technologies are continuously evolving. The Internet is probably the most complex system ever created (Kraus, Stricker & Speyer, 2010; Schneier, 2004). Salman (2014) viewed Internet as the most vibrant mass media of the century that attracts everyone. Cohen-Almagor (2011) and Dowland, Furnell, Illingworth and Reynolds (1999) claimed that the rapid growth of the Internet has had impacts on our everyday lives. Malaysians are also not excluded from the rapid advancement in technology as their lives are increasingly relying on the Internet to accomplish their daily chores (DAKA Advisory, 2014). The number of Internet users are ever increasing in Malaysia. Malaysian Communications and Multimedia Commission (2014) reported that the Internet penetration rate among Malaysians in the first quarter of 2014 as 67.3%. Although the country had benefited from the advancement in Internet technology, the ever-increasing cyber security incidents are worrying.

The cyberspace is as dangerous as physical space and may probably be more dangerous as cyberspace provides anonymity for its users (Yar, 2013). Moreover, the cyberspace involves faceless and borderless communication. According to LeFebvre (2012), the Internet was designed as an open system for trustworthy users but it has turned to become a vulnerable space due to its rapid growth. Globalization and technological advancement had made cyberspace vulnerable to various types of threats

(El Kettani & Debbagh, 2008; Frank & Odunayo, 2013). As the number of Internet users and technology grows, cyber threats are also skyrocketing (Abd Rahim, et al., 2015; Furnell, 2002; Muniandy & Muniandy, 2012). Siponen (2001) and Yar (2013) considered the Internet as a dangerous and lawless zone with undesirable activities that are ever increasing. Siponen (2001) and Vrana (2012) cited the advancement and availability of newer technologies, cheaper costs, the increasing number of unsuspecting and vulnerable users and easily transferable knowledge as the main culprits for transforming cyber space into a vulnerable space.

Cyber security countermeasures are being implemented through technological, non-technological methods and legislation (Furnell, 2002; Muniandy & Muniandy, 2012; Schneier, 2004). Howard and Prince (2011) agree that we have the necessary and the required technology to protect even the most complex network. However, Howard and Prince (2011) and Schneier (2004) argued that the interaction of humans with technology is the reason for the failure of technological countermeasures. Munir and Yasin (2010) claimed that cyber laws enacted by governments to protect netizens failed as there are other requirements, such as homogenous international laws, investigations based on evidence and cross border cooperation that are obligatory to ensure a successful implementation. A lack of tech-savvy enforcement officers further affect the chances for a cyber-criminal from being prosecuted based on the enacted cyber laws. Furnell (2002) and Yar (2013) admitted the difficulties in implementing and enforcing legislations across the globe.

Non-technological countermeasures are provided through training and education to address the human factors that are involved in cyber security. Cyber security awareness training and education is important for cyberspace users to protect themselves from cyber threats (Al-Shehri & Clarke, 2012; Furnell, 2002; LeFebvre, 2012; Siponen, 2001; Stephanie, 2005; Thomason, 2013). Al-Shehri and Clarke (2012) claimed that the human factor in information security must be addressed through education to ensure that the general population are aware of security threats. Therefore, it is vital that the human factor in cyber security is attended properly to safeguard the Malaysian cyberspace. Thus, this study is addressing the cyber security issues by educating users.

1.2 Background of the Problem

As identified by Paynter and Lim (2001) and Salman, Choy, Wan Mahmud and Abdul Latif (2013), the Internet age in Malaysia began in the year 1995. Paynter and Lim (2001) reported that the first Internet study was conducted in Malaysia from October to November 1995, it was found that one out of every one thousand Malaysians had access to the Internet, which translated to 20,000 Internet users out of the then total population of 20 million.

In 1998, the percentage of Internet users grew up to 2.6% of the total population (Paynter & Lim, 2001). Muniandy and Muniandy (2012) reported that after the year 2000, Internet penetration in Malaysia continued to grow rapidly. As shown in Table 1.1, Internet users in Malaysia are growing rapidly, where in 1995, the number of Internet users stood at only 0.1% and within 10 years this grew up to 37.9%. As of 2013, Internet penetration rate in Malaysia was at 67.0%. The Internet usage in Malaysia shows a sharp increase and grows exponentially from the year 1998 until now, and is expected to grow more in the future. All the preceding findings indicate that Internet penetration is increasing rapidly in Malaysia but is the cyberspace fully protected?

Table 1.1

Internet Users, Total Population and the Percentage of Internet Users in Malaysia

Year	Internet Users	Total Population	%
2000	3,700,000	24,645,600	15.0
2005	10,040,000	26,500,699	37.9
2006	11,016,000	28,294,120	38.9
2007	13,528,200	28,294,120	47.8
2008	15,868,000	25,274,133	62.8
2009	16,902,600	25,715,819	65.7
2010	16,902,600	26,160,256	64.6
2012	17,723,000	29,179,952	60.7
2013	20,140,125	30,073,353	67.0
2016*	21,090,777	20,751,602	68.6

Note. *. Estimate for July 1, 2016. Adapted from Internet World Stats Institution, 2012; Internet World Stats Institution, 2014b; Internet Live Stats, 2017.

Based on a report by AFP (2014), cyber security has grown into a global industry that is worth around half a trillion dollars and continuing its growth steadily. The report also claims that the global economic costs of cyber-attacks is at $445 billion causing 350,000 job losses in the United States and Europe alone. The authors estimated the losses due to cybercrime to be in the range of $375 billion to $575 billion and they have agreed that these figures could be higher than the reported losses due to limited data from around the world. The report also stated that more than 800 million individuals’ data were stolen in the year 2013 alone.

Gan, Ling, Yih and Eze (2008) claimed phishing attacks and identify theft as an obstacle for the growth of online banking in Malaysia as the number of attacks launched on financial institutions had continuously increased since the year 2000. Hamudin and Ariffin (2014) reported that Sophos Security Threat Report 2013 exposed Malaysia as the sixth most vulnerable country targeted for cybercrimes and purportedly lost RM1 billion to cybercrimes. Citing the reports by Malaysia Computer Emergency Response Team (MyCERT), the authors also reported that cybercrime in Malaysia has increased from 9,986 cases in 2012 to 10,636 cases in 2013.

Gupta, Kuppili, Akella and Barford (2009) found that malware attacks on the Internet is rising and evolving rapidly with new types of vulnerabilities, attacks and more sophisticated malicious codes. APWG (2014) reported that 32.7% of personal computers around the globe were infected with malicious software. According to Garnaeva, Chebyshev, Makrushin, Unucheck and Ivanov (2014), Malaysia was at the ninth position for top 10 countries with the most number of attacked users through malware. Also, Malaysia was placed at tenth for top 10 countries with high risk of infection with malware. Ramendran (2014) reported that a malware known as Zeus is being used in phishing attacks targeting smartphone and tablet users who perform online banking activities. It was reported that eight victims have lost approximately RM 60,000. Similarly, Malaysia was shocked when some hackers stole about RM3 million by hacking into automated teller machines (ATM) (Cheng, 2014). Police reported that these hackers used a virus known as “ulssm.exe” to accomplish their crime.

In a report published in *the Sun* newspaper (August 28, 2013), during the first seven months of 2013, RM1.07 billion was recorded in losses from thousands of various scams, corporate fraud and other commercial crimes. It was also reported that Malaysia was positioned in the sixth place of being at high risk for online fraud and malware attacks. Most of these cyber security incidents targeted young Internet users (Ramendran, 2013).

Increasing number of cyber incidents were due to the rapid increase in the number of Internet users. However, Yar (2013) acknowledged that there was massive underreporting of cybercrimes. As pointed out by Dowland et al. (1999), the real level of computer crimes is higher than those reported as some organizations do not want the risk of undesirable consequences such as bad publicity, legal liability and loss of customers. These researchers have also acknowledged that it is difficult to determine the exact number of affected domestic computer users due to cyber security incidents. Augastine (2007) claimed that only 10% of cyber incidents were reported, while Furnell (2002) and Kshetri (2010) found that less than 10% of cybercrimes are ever reported to the relevant authorities. Thus, the researcher strongly agrees that the current state of cyber security in Malaysia is worse than what has been reported.

Ciampa (2010) stated that providing cyber security had become a real challenge since both the number of attacks and the difficulties in defending against these attacks are ever increasing. As elaborated by Gallaher, Link and Rowe (2008), technology and tools are freely available for both security professionals and attackers to protect cyberspace and to launch the attacks on the vulnerabilities of cyberspace. Security experts believe that system security fails miserably when it involves humans. As espoused by Howard and Prince (2011), technology is not responsible for IT security failure but human communication with technology initiates security issues. Another security expert, Schneier (2004) stated that “people often represent the weakest link in the security chain are chronically responsible for the failure of security systems” –

p.255. To conclude, technology can only function properly if the human factor in the cyber security can be handled successfully.

Thomason (2013) claims that user behaviour towards cyber security must be changed to allow the users to be aware of existing cyber threats. This can be accomplished by using technology combined with education to help users understand and follow security requirements. Siponen (2001) stated that the general public must be aware of information security issues. In addition, Al-Sheri (2012) considered cyber security as a general knowledge for those in this era. Parsons, McCormac, Butavicius and Ferguson (2010) meanwhile, claimed that users must be educated about the importance of security awareness and these programs must incorporate behavioural training.

Cyber security awareness training must help the user to be up-to-date with the knowledge required to identify or know the methods of assessing computer systems vulnerabilities, and have knowledge of a source that will be able to assist them when they face problems (Trim & Upton, 2013). Training and education is vital for improving user awareness towards cyber security issues (Bada & Sasse, 2014; Dodge, Carver, & Ferguson, 2007; Eminagaoglu, Ucar, & Eren, 2009; Furnell, Bryant & Phippen, 2007; Siponen, 2001; Stephanie, 2005). Dupuis (2017) reported that users' risky cyber security behaviour were influenced by their lack of knowledge, skills and abilities. Malmedal and RØislien (2016) claimed that people who are educated in cyber security aspects behave more securely on the Internet. Hunt (2016) declared that cyber security awareness is more important for the current time than it has ever been in the past.

Past surveys showed that Malaysians generally lack cyber security awareness. A study by Norton Cybercrime in 2011 revealed that seven out of ten Malaysian adults thought they are more likely to be victims of physical crime rather than cybercrime (Timbuong, 2011). A study conducted at the International Islamic University Malaysia (IIUM) found that students are generally lacking in cyber security awareness and are more susceptible to social engineering attacks (Adam, Yusra al-Amodi & Ibrahim, 2011). Ishak et al., (2012) conducted a research to assess the Malaysian social networking users' awareness level and categorized the findings based on gender and education level. The researchers found that male and less educated respondents have a lower awareness level regarding their usage of social networking sites.

The surveys mentioned above show that Malaysians did not expect the cyberspace to be dangerous and consequently cyber security awareness among the people is also low. According to Cisco (2010) and DAKA Advisory (2014) cyber security awareness among all types of users are vital in protecting themselves from the growing cyber security threats. Therefore, Malaysian government had taken many initiatives to protect its citizens as well as its entities from cyber threats. One of such method is to educate and enhance cyber security awareness of the general public through 'CyberSecurity Awareness For Everyone' (CyberSAFE). CyberSAFE was setup by CyberSecurity Malaysia, an agency of Ministry of Science, Technology and Innovation (MOSTI). CyberSAFE provides practical knowledge and vital information to the general people in protecting themselves from the danger of online (CyberSecurity Malaysia, 2010).

The researcher had analyzed the CyberSAFE Malaysia's official website at http://www.cybersafe.my/en/. The researcher had found that CyberSAFE Malaysia addressed four categories of people, namely, kids, youth, parents as well as organisations in their cyber security education and awareness programmes. These cyber security education materials are presented to the intended audiences in an unstructured method. The materials are arranged according to captions for the people. People can access and read the materials by clicking on any of these captions. The researcher further analyzed some Malaysian banks' websites that provide online banking services. These websites also presented their cyber security materials in an unstructured method. However, Malaysians usually study in a structured method, whereby the learning materials are presented in a systematic way. Lee, Sudweeks, Cheng and Tang (2010) categorized Malaysian students as individuals who preferred to be guided in their learning process, adopted a less analytic approach in learning and expected more instructional assistance in seeking for information that would helped them in their learning process.

Katuk and Zakaria (2015) reported that both structured and unstructured methods were widely employed in web-based instruction. These researchers claimed that both of these methods have their own advantages and disadvantages. Structured (linear navigation) facilitates students to learn in a systematic way while limiting students' controls over the contents. These researchers also reported that unstructured method (non-linear navigation) widely used in web-based instruction. The unstructured method while giving the students greater control over the contents, causing some students unable to manage the high level of control given by this unstructured method.

Therefore, this research trained the participants of the study using two modes of training modules, structured versus unstructured, and assess the effectiveness of these modules on participants' cyber security awareness and their perceived cyber security behaviour. The training modules were used to educate users on issues such as social engineering attacks and password setting. The social engineering attacks further divided into 4 main aspects, namely, phishing, malware, online scam and other social engineering issues. The two modes of training modules, namely, structured and unstructured, consist of five main modules each. Structured online training module's contents were presented in a linear style, in which, all sub modules of the five main modules were prearranged by the researcher. Respondents were required to navigate and learn the materials in that sequence. Conversely, in unstructured online training module, the five main modules were divided into submodules according to their subtopics. Respondents were given the option to select any submodules to learn in any order. Contents of both of these modules were the same.

This research also studied the interaction effects of structured and unstructured cyber security training modules on types of motivation and specialization of study areas of participants in changing their awareness and perception on behaviour towards cyber security issues.

Antwi-Bekoe and Nimako (2012) have chosen students from Information Technology Education and Department of Computer Science only, for their cyber security awareness study. The rationale was due to the respondents' familiarities with the cyber security aspects which would enable them to provide accurate responses. Mensch and Wilkie (2011) studied the information security attitudes, behaviours and tools usage of nine different academic majors and found that respondents from both information technology and also fine arts received some of the highest scores, while surprisingly respondents from criminology scores lowest mean security behaviour scores. Muhirwe and White (2016) considered students' major as one of their control variable in their study. These researchers categorized students' major as technical and non-technical. Their study findings showed that students' major or gender, age, academic status and years of computing did not influence students' cyber security practice. However, cyber security awareness training positively influence awareness and subsequently the respondents' practice. In relation to the above discussions, past studies have shown conflicting results on the role of specialization areas on the students' cyber security awareness and behaviour.

In line with the above discussions, students' specialization areas (major) should be explored as a variable which could influence the strength of the training modes on the cyber security awareness and perceived behaviour. Furthermore, the study was conducted in a college, where the students are categorized according to their specialization areas. Thus, the respondents' specialization areas was considered as one of the moderating variable to understand the effects of training mode on their cyber security awareness and perceived behaviour. In addition to that, generally students at higher education institutions were considered as heavy Internet users, irrespective of their specialization areas. The study findings would be able to provide a breakthrough to understand higher education students' cyber security awareness and perceived behaviour and facilitate the curriculum planning of different specialization areas in the future.

Clayton, Blumberg and Auld (2010) considered learner's motivation correlated with successful learning. Rakes and Dunn (2010) claimed that lack of motivation among students at all levels is being considered as a problem in the learning process. Chen and Jang (2010) claimed that self-determination theory is an appropriate framework for addressing motivation aspects in online learning environment. Self-determined motivation has been associated to diverse educational outcomes from early elementary school to students at higher education institutions (Deci, Vallerand, Pelletier & Ryan, 1991). According to Chen and Jang (2010), Harnett (2016), Harnett, St. George and Dron (2011) as well as Sansone, Fraughton, Zachary, Butner and Heiner (2011) motivation is one of the important factor that should be considered in the online learning environment. Thus, the researcher considered motivation as one of the moderating variable of the current study since respondents were trained in the online environment.

1.3 Problem Statement

Schneier (2004) and Yar (2013) claimed that the cyberspace is more vulnerable than the physical world because of the borderless, virtual and faceless communications that are involved. As explained by Wechuli, Muketha, and Mateko (2014) and Yar (2013), the development of the Internet and its related technologies brought greater evolution in the types of crimes that can be launched. Howard and Prince (2011) and Schneier (2004) claimed that the Internet enables devastating cyber security threats to be launched on a bigger scale. Cybercrimes are ever increasing due to the advancement in the technology coupled with the increasing number of Internet users (Furnell, 2002; Siponen, 2001; Wechuli et al., 2014). Furnell (2002) and Wechuli et al. (2014) claimed that the growing number of reported cyber security incidents show that cybercrimes are worsening.

Protection through technology alone had failed to reduce the growing cyber security threats (Howard & Prince, 2011; Safa et al., 2015; Schneier, 2004; Talib, Clarke, & Furnell, 2010). Legislations have failed to address the increasing cybercrimes (Furnell, 2002; Munir & Yasin, 2010; Yar, 2013). Security experts believe that the weakest link in an information system is human factor. Addressing the human factor is necessary to solve many security issues especially those related to aspects that involve human interaction with Information systems (Ciampa, 2010; Howard & Prince, 2011; Mitnik & Simon, 2005; Safa et al., 2015; Schneier, 2004; Whitman & Mattord, 2009). Education is vital to increase the awareness level (Abd Rahim, et al., 2015; Forcht, Pierson, & Bauman, 1988; Siponen, 2001). According to Moore (2011), it is important to educate potential victims to the dangers of Internet. Sheng, Holbrook, Kumaraguru, Cranorm and Downs (2010) reported that education materials indeed play a pivotal role in reducing user tendencies to reveal personal information in cyber security incidents such as phishing. Thus, this study attempts to provide awareness and improve Internet users' perceived behaviour by training them using cyber security training modules.

Personal Internet users or common users are highly susceptible to security threats (Furnell, et al., 2007; Howe, Ray, Roberts & Urbanska, 2012). They are easy targets for security threats due to a lack of cyber security awareness and knowledge (Furnell, Valleria & Phippen, 2007; Howe et al., 2012; Kritzinger & von Solms, 2010). Kritzinger and von Solms (2010) claimed that a lack of up to date security awareness information is one of the contributing factors for the victimization of home users. There is limited research on the development of awareness training programmes for personal Internet users as most of the research are focused on training programmes for organization's employees (Kritzinger & von Solms, 2010; LeFebvre, 2012; Li & Siponen, 2011; Talib et al., 2010). The available security awareness programmes for personal Internet users are mostly accessible online, containing incomplete and out-of-date information, not easily searchable by novice users, and a lack of interaction with users (Kritzinger & von Solms, 2010). Limited research has been done to measure the effectiveness of security awareness training programmes on users (Ng, Kankanhalli, & Xu, 2009; Talib et al., 2010).

The study targeted college students, aged 18-21 years old, under the young adult category. This is due to the factor that the number of Malaysian young adults accessing the Internet and the total amount of time spent by them on the Internet is increasing rapidly (Marketing Magazine, 2011). In the Malaysian context, those in the age group of 18-24 years old are pursuing their tertiary education, thus the study focuses on college students. Vrana (2012) claimed that the current generations of students are heavy Internet users. Students at tertiary education level are also more vulnerable to cyber security threats as most of their daily communication and education related activities are performed on the Internet (Abolarinwa, Tiamiyu & Eluwa, 2015; Masrom, Ismail & Hussein, 2008; Mensch & Wilkie, 2010). Rezgui and Marks (2008) and Sheng et al. (2010) reported that young adults, in the age group of 18-24 years old are more susceptible to cyber security threats.

Moreover, Rezgui and Marks (2008) claimed that universities are among the least secure environment in terms of information systems as only a small percentage of tertiary education institutions conduct security awareness training for their students and staff. Since the study is conducted at a higher education institution, the respondent’s motivation types and specialization areas were considered as moderator variables. Considering all the existing constraints in the current context, this study investigated the effectiveness of structured and unstructured cyber security training modules on the users.

1.4 Research Objectives

The main objectives for this research are as follows:

1. To design and develop two modes of online cyber security training modules (structured and unstructured) related to human factors.
2. To determine whether structured or unstructured mode of presentation is better in developing awareness and perceived behaviour on the cyber security threats among college students.
3. To investigate the effects of structured versus unstructured cyber security training module on cyber security awareness and perceived behaviour of college students who are intrinsically and extrinsically motivated.
4. To investigate the effects of structured versus unstructured cyber security training module on cyber security awareness and perceived behaviour among college students from technical and non-technical specialization areas.

1.5 Research Questions

This study seeks to answer the following research questions: -

1. Is there a significant difference in cyber security awareness between students trained using structured versus unstructured online cyber security training module?
2. Is there a significant difference in perceived cyber security behaviour between students trained using structured versus unstructured online cyber security training module?
3. Is there a significant interaction effect of the types of online cyber security training modules (structured versus unstructured) and the types of student motivation (intrinsic versus extrinsic) on students' cyber security awareness?
4. Is there a significant interaction effect of the types of online cyber security training modules (structured versus unstructured) and the types of student motivation (intrinsic versus extrinsic) on students' perceived cyber security behaviour?
5. Is there a significant interaction effect of the types of online cyber security training modules (structured versus unstructured) and the students' specialization areas (technical versus non-technical) on students' cyber security awareness?
6. Is there a significant interaction effect of the types of online cyber security training modules (structured versus unstructured) and the students' specialization areas (technical versus non-technical) on students' perceived cyber security behaviour?

1.6 Research Hypotheses

The hypotheses for this study are formulated as null hypotheses. The null hypotheses that relate to the research questions are as follows:

H_{01} There is no significant difference in cyber security awareness between students trained using structured versus unstructured online cyber security training module.

H_{02} There is no significant difference in perceived cyber security behaviour between students trained using structured versus unstructured online cyber security training module.

H_{03} There is no significant interaction effect of the types of online cyber security training modules (structured versus unstructured) and the types of student motivation (intrinsic versus extrinsic) on students' cyber security awareness.

H_{04} There is no significant interaction effect of the types of online cyber security training modules (structured versus unstructured) and the types of student motivation (intrinsic versus extrinsic) on students' perceived cyber security behaviour.

H_{05} There is no significant interaction effect of the types of online cyber security training modules (structured versus unstructured) and the specialization areas (technical versus non-technical) of students on students' cyber security awareness.

H_{06} There is no significant interaction effect of the types of online cyber security training modules (structured versus unstructured) and the specialization areas (technical versus non-technical) of students on students' perceived cyber security behaviour.

1.7 Theoretical Framework

Figure 1.1 illustrates the theoretical framework of this study. One of the dimensions of cognitive style is Holist-Serialist which was identified by Pask (1976). This cognitive style dimension is applied in the development of cyber security training modules for this research. Structured online training module was developed based on the serialist approach, while unstructured online training module was created based on the holist approach. Though there are three types of cognitive load, the study explores extraneous load in Cognitive Load Theory (Sweller, 1994) as the two types of online training modules involved different ways of information presentation to respondents of the study. Two constructs, threat appraisal and coping appraisal in Protection Motivation Theory by Rogers (1975) and Rogers, Cacioppo and Petty (1983) were incorporated into the structured and unstructured online training module to study the effects of fear appeal on student's behaviour. Furthermore, Krathwohl's Taxonomy of the Affective domain by Krathwohl, Bloom and Masia (1964) was used to study the effects of these modules on the student's awareness level.

The Self-Determination Theory (SDT) is a macro-theory of human motivation, personality development and well-being which was developed by Ryan and Deci. SDT focuses on the degree to which human behavior is self-motivated and self-determined. The theory describes intrinsic motivation and the four variations of extrinsic motivation.

McCumber Cube (1991) provides a graphical representation of the architectural approach widely used in computer and information security. If extrapolated, the McCumber Cube shows that 3 dimensions of each axis becomes 3x3x3 cube with 27 cells representing areas that must be addressed to secure today's information security (Whitman & Mattord, 2009). Hafiz and Johnson (2006) claimed that McCumber Cube comprises of three building blocks, namely, (1) information states – transmission, storage, processing; (2) critical information characteristics – confidentiality, integrity, availability; and (3) security measures – technology, policy and practices and education, training and awareness (or human factor). All of the above mentioned theories and models were used to explain the importance of analyzing cyber security countermeasures through human aspects.

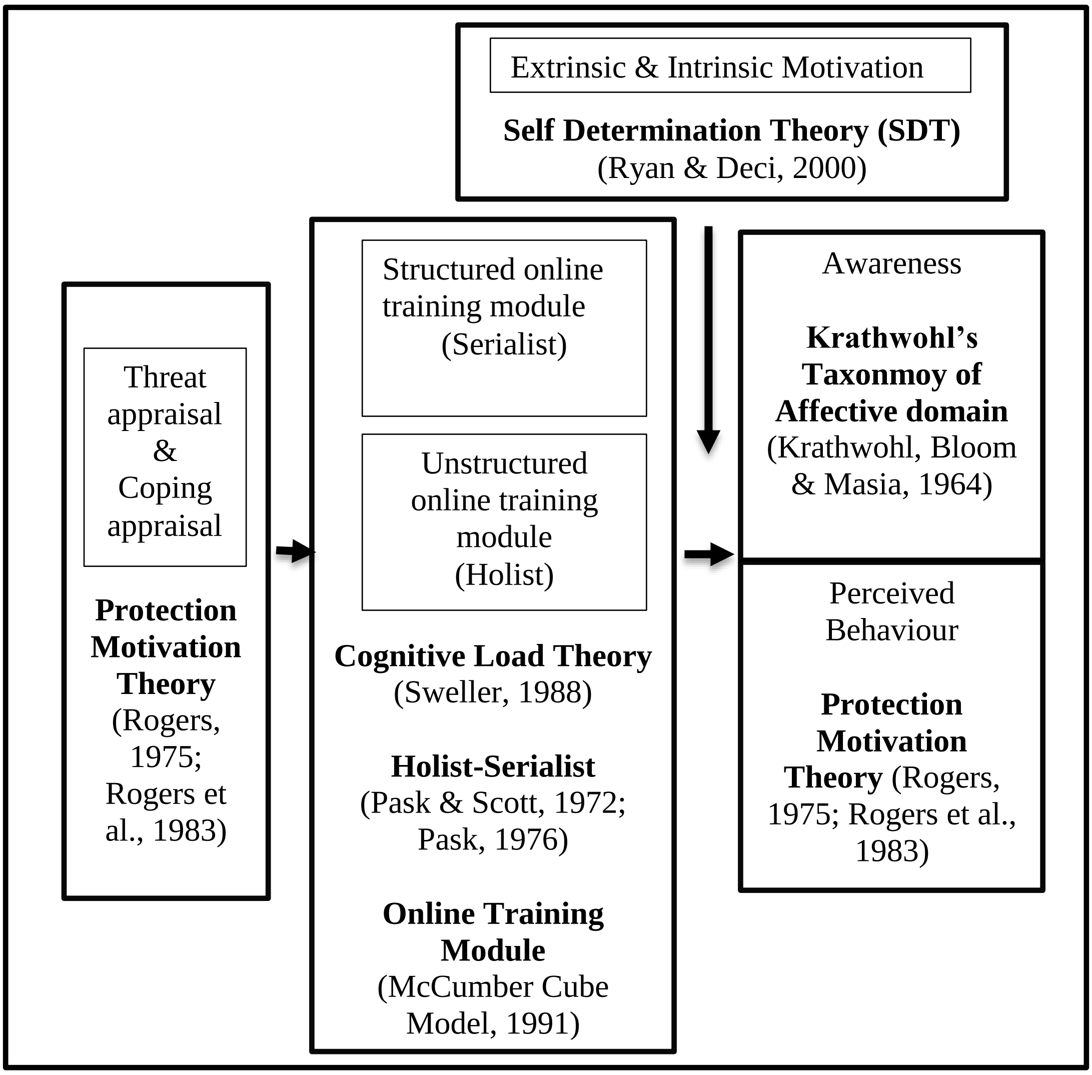
Extrinsic & Intrinsic Motivation
Self Determination Theory (SDT)
(Ryan & Deci, 2000)
Threat appraisal & Coping appraisal
Protection Motivation Theory (Rogers, 1975; Rogers et al., 1983)
Structured online training module (Serialist)
Unstructured online training module (Holist)
Cognitive Load Theory (Sweller, 1988)
Holist-Serialist (Pask & Scott, 1972; Pask, 1976)
Online Training Module (McCumber Cube Model, 1991)
Awareness
Krathwohl's Taxonmoy of Affective domain (Krathwohl, Bloom & Masia, 1964)
Perceived Behaviour
Protection Motivation Theory (Rogers, 1975; Rogers et al., 1983)

Figure 1.1. Graphical representation of theoretical framework.

1.8 Research Framework

Figure 1.2 illustrates the research framework of this study. The independent variables (IV) identified for this research are two types of learning modules: structured online training module and unstructured online training module. There are two moderator variables (MV), motivation (intrinsic and extrinsic) and specialization areas (technical and non-technical). Dependent variables are respondents' cyber security awareness level and their perceived behaviour. This research aims to identify the influence of structured and unstructured online training module on the students' cyber security awareness and their perceived behaviour using the students' motivation types and specialization areas as moderator variables.

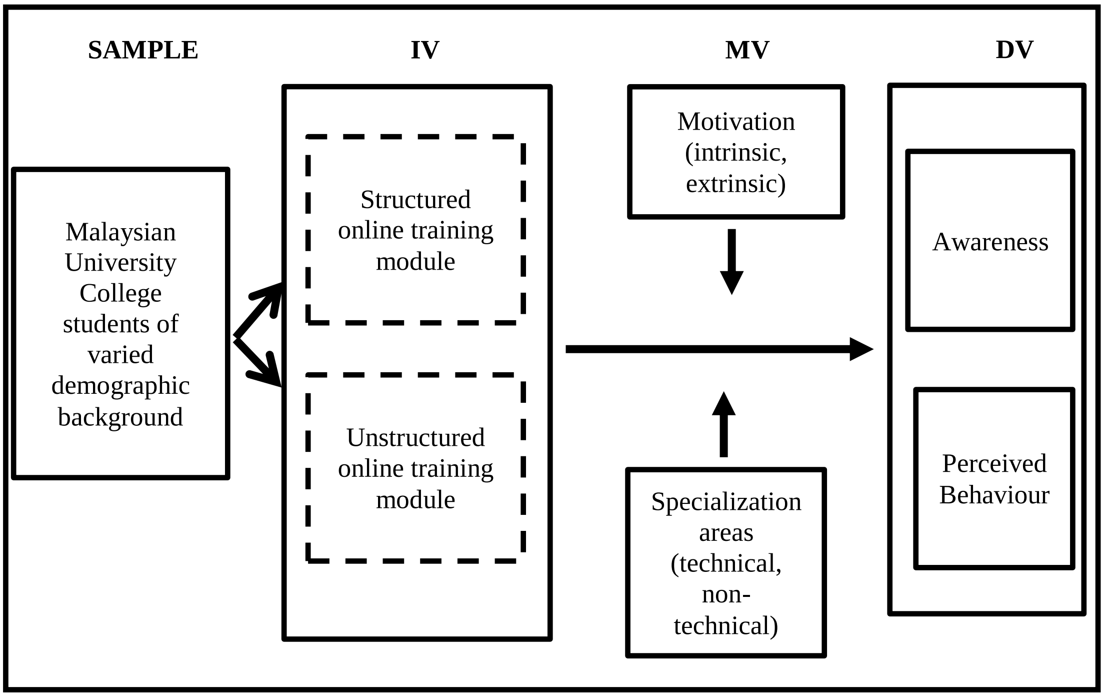
SAMPLE
IV
MV
DV
Malaysian University College students of varied demographic background
Structured online training module
Unstructured online training module
Motivation (intrinsic, extrinsic)
Specialization areas (technical, non-technical)
Awareness
Perceived Behaviour

Figure 1.2. Research framework.

1.9 Significance of the Study

As of June 2016, Malaysia had 21 million Internet users for a population of 30.75 million. This number is increasing and the cyber threats in Malaysian cyberspace are also skyrocketing. Even though cyber security threats are common among all types of Internet users, this study focused only on higher education students. The rationale of selecting higher education students as study participants was due to their long hours of exposure to Internet as well as their potential to be the future workforce of Malaysia.

The study investigated the effects of structured versus unstructured online training modules on college students' cyber security awareness and perceived behaviour. Students' specialization areas and motivation types were considered as moderating factors of the study. The study would identify the variation effects of structured versus unstructured online training module on intrinsically and extrinsically motivated students. The study also would identify how the technical and non-technical students differ in their cyber security awareness and perceived behaviour after the self-training. Hence, if the study does identify that there are differences among intrinsically and extrinsically motivated students as well as technical and non-technical students, the future cyber security education programmes can be tailored according to the users' needs.

The research findings could be used by relevant administrators and government bodies to identify the current state of awareness and perceived cyber security behaviour among Malaysian higher education students and enable them to initiate appropriate measures to address the problems effectively.

The study findings also highlighted the importance of providing a proper cyber security education for students. The higher education institutions as well as national and private schools would be enlightened about the importance of redesigning their curriculum by incorporating cyber security as one of the components.

Moreover, the contents of the training module could be tailored and incorporated into the syllabus of primary, secondary and tertiary education. The contents of the module could also be used in preparing campaigns to educate the general public regarding the uncertainty that exists in cyberspace.

In a nutshell, the study would be the first step to bring realization into introducing cyber security education as part of the Malaysian education system.

1.10 Limitations of the Study

The research focuses on the cyber security awareness and perceived behaviour among higher education students in Malaysia and to determine the best mode to educate Internet users. The following are the limitations of this study:

(i) One of the limitations was that the research focused on students in the selected college only. Although there are several branches of the selected private university college all over Malaysia, due to time, cost, and distance constraints, both structured and unstructured training modules were tested only in the chosen branch.

(ii) The structured and unstructured online training module were tested in the same college, as such communications between these groups were expected. This limitation was addressed by enabling both online training modules only for ~5 hours per day. The rationale for enabling these online training modules for five hours was to give ample time for the samples to access the contents as the study was conducted during their semester period.

(iii) A sample size of 240 university college students was used for the purpose of this study. As such, the results of this study cannot be generalized to all the students pursuing tertiary education in other varsities in Malaysia.

(iv) Internet users in Malaysia come from different age groups. But the study specifically focuses on young adults in the age range of 18 to 21 years. Thus, the results of this study cannot be generalized to the whole Malaysian population.

(v) The respondents' perceived behaviour changed were measured by using an instrument only and not by observation. Furthermore, the respondents' awareness and perceived behaviour were measured immediately after the treatment. Thus, the effects of these online training modules on the respondents perceived behaviour on longer term could not be established.

(vi) Respondents' specialization areas were grouped into two main categories only, namely, technical and non-technical and not analyzed individually. Therefore, the strength of the specific specialization areas of the students on the online training modules could not be established.

1.11 Definitions of Operational Terms

The following are the definitions of some of the key terms or variables used in this study:

1.11.1 Awareness

According to online Cambridge Dictionary (2017), awareness is defined as "knowledge that something exists, or understanding of a situation or subject at the present time based on information or experience." Awareness in the current study refers to end users' level of understanding of cyber security incidents and the degree of responsiveness regarding the existence of cyber security threats.

1.11.2 Perceived Behaviour

Online Cambridge Dictionary (2017) defined perceived as to belief something and behaviour as the way a person behaves in particular situation. In the current study's context perceived behaviour refers to the apparent end users' practices and actions on the cyberspace.

1.11.3 Cyber security

According to ITU (n.d.) cyber security "is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" – p.43. Cyber security refers to