

2014

PERSONALISING INFORMATION SECURITY EDUCATION

Talib, Shuhaili

<http://hdl.handle.net/10026.1/2896>

<http://dx.doi.org/10.24382/4735>

University of Plymouth

All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.

COPYRIGHT STATEMENT

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without the author's prior consent.

Copyright © 2014 Shuhaili Talib

PERSONALISING INFORMATION SECURITY EDUCATION

by

SHUHAILI TALIB

A thesis submitted to Plymouth University
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing and Mathematics
Faculty of Science and Technology

January 2014

Abstract

Personalising Information Security Education

Shuhaili Talib

Whilst technological solutions go a long way in providing protection for users online, it has been long understood that the individual also plays a pivotal role. Even with the best of protection, an ill-informed person can effectively remove any protection the control might provide. Information security awareness is therefore imperative to ensure a population is well educated with respect to the threats that exist to one's electronic information, and how to better protect oneself.

Current information security awareness strategies are arguably lacking in their ability to provide a robust and personalised approach to educating users, opting for a blanket, one-size-fits-all solution. This research focuses upon achieving a better understanding of the information security awareness domain; appreciating the requirements such a system would need; and importantly, drawing upon established learning paradigms in seeking to design an effective personalised information security education.

A survey was undertaken to better understand how people currently learn about information security. It focussed primarily upon employees of organisations, but also examined the relationship between work and home environments and security practice. The survey also focussed upon understanding how people learn and their preferences for styles of learning. The results established that some good work was being undertaken by organisations in terms of security awareness, and that respondents benefited from such training – both in their workplace and also at home – with a positive relationship between learning at the workplace and practise at home.

The survey highlighted one key aspect for both the training provided and the respondents' preference for learning styles. It varies. It is also clear, that it was difficult to establish the effectiveness of such training and the impact upon practice. The research, after establishing experimentally that personalised learning was a viable approach, proceeded to develop a model for information security awareness that utilised the already successful field of pedagogy and individualised learning. The resulting novel framework "*Personalising Information Security Education (PISE)*" is proposed.

The framework is a holistic approach to solving the problem of information security awareness that can be applied both in the workplace environment and as a tool for the general public. It does not focus upon what is taught, but rather, puts into place the processes to enable an individual to develop their own information security personalised learning plan and to measure their progress through the learning experience.

Contents

List of Figures.....	iv
List of Tables.....	vi
Abbreviations	viii
Acknowledgement.....	xi
Authors Declaration.....	xii
1 Introduction	1
1.1 Aim and objectives	3
1.2 Thesis structure	3
2 A Review of Information Security Awareness and Practices	5
2.1 Introduction	5
2.2 The importance of information security awareness	5
2.3 Information security awareness.....	8
2.4 Security Awareness.....	11
2.4.1. Information Security Awareness at University of Missouri and Aetna.....	12
2.4.2 Security Awareness for Home users.....	14
2.5 Conclusion.....	20
3 An Information Security Awareness Survey.....	21
3.1 Purpose of the survey.....	21
3.2 Research method	22
3.3 Methodology of the survey	22
3.4 Validation of the survey	25
3.5 Filtering mechanism	26
3.6 Survey findings	28
3.6.1 Demographics.....	28
3.6.2 Information security awareness level.....	32
3.6.3 Information security practices at workplace	40
3.6.4 Information security practices at home	50
3.6.5 Effectiveness of information security training.....	59
3.7 Conclusion.....	71
4 Education and Learning Practices	77
4.1 Introduction.....	77
4.2 Information security awareness and practices through education.....	78
4.3 Learning styles	80
4.3.1 Learning styles in adult education.....	83

4.3.2 Human Sensory Learning Styles	85
4.3.3 VARK Learning Styles	87
4.3.4 Critique about learning styles.....	89
4.4 Personalised learning	90
4.4.1 Challenges in implementing personalising learning.....	97
4.4.2 Benefits of personalising learning	98
4.5 Implementation of the personalised learning.....	99
4.6 Models of Personalised Learning	100
4.6.1 Personalised Collaborative Skills for student Model (CDSM).....	100
4.6.2 Conceptual model for construction	104
4.6.3 Personalised learning system based on Solomon Learning Style	106
4.7 Conclusion.....	108
5 An Investigation into Improving Information Security Practices through Personalised Learning ...	109
5.1 Introduction.....	109
5.2 Methodology.....	109
5.2.1 Research design.....	109
5.2.2 Preliminary study report 1	114
5.2.3 Preliminary study report 2	117
5.3 Study on the effectiveness of learning styles upon learning information security topic (Main study).....	122
5.4 Results.....	124
5.4.1 Demographics.....	124
5.4.2 Analysis based on VARK classification.....	126
5.4.3 Further Analysis	132
5.5 Discussion	138
5.6 Conclusion.....	139
6 The Personalising Information Security Education (PISE) Framework.....	140
6.1 Introduction.....	140
6.2 System Requirements	140
6.3 PISE Model.....	141
6.4 PISE Implementation.....	148
6.4.1 Private PISE.....	149
6.4.2 Public PISE	159
6.4.3 PISE System Prototype	168
6.5 PISE Evaluation and Discussion	181
6.6 Conclusion.....	182

7 Conclusion and Future Works.....	184
7.1 Achievements	184
7.2 Limitations	186
7.3 Future research	187
7.4 The future of information security education	188
References.....	189
Appendix A.....	I
Faculty of Technology Ethical Approval Application Form	I
Appendix B.....	I
The Transferability of Information Security Knowledge Survey.....	I
Appendix C.....	XIV
The First Version of Survey Questions.....	XIV
Appendix D.....	XXVI
The Survey Results	XXVI
Appendix E.....	XLIII
Pre-test Questions Version 1.....	XLIII
Appendix F	XLIX
Learning materials	XLIX
Appendix G	LXIII
Answer Key To The Pre-test Version 1	LXIII
Appendix H.....	LXV
Pre-test Questions Version 2.....	LXV
Appendix I	LXXII
Answer Key to Pre-test Version 2.....	LXXII
Appendix J	LXXIV
Faculty of Science and Technology Ethical Approval of Research Involving Human Participants	LXXIV
Appendix K.....	CIX
VARK Questionnaire	CIX
Appendix L	CXV
User Experience Survey.....	CXV
Appendix M	118
Expert Evaluation	118
Appendix N.....	122
Publications	122

List of Figures

Figure 1 Survey respondents by age range	28
Figure 2 Respondents by their highest level of education	29
Figure 3 Respondents by their size of organisation	31
Figure 4 Respondents by their primary role within the organisation	32
Figure 5 Information security awareness level	33
Figure 6 Respondents by their Internet/computing skills	34
Figure 7 Respondents' information security awareness level and Internet/computing skills	34
Figure 8 Percentage of total respondents about who they think is responsible for information security tasks	35
Figure 9 Security term 'Phlopping' and respondents' security awareness level	38
Figure 10 Security term 'Whooping' and respondents' security awareness level (in percentage) ...	39
Figure 11 Security term 'Whooping' and respondents' security awareness level (in percentage)	39
Figure 12 Respondents by information security training provided in their organisation	40
Figure 13 Percentage of respondents by frequency of attending security training	41
Figure 14 Percentage of respondents by experienced training methods	43
Figure 15 Respondents by their preferences for having information security training	48
Figure 16 Percentage of respondents who answered 'Always' to the above statements (at workplace)	49
Figure 17 Percentage of respondents who answered 'Never' to the above statements (at workplace)	50
Figure 18 Respondents by how frequent they read about information security at home	53
Figure 19 Respondents by their opinion on giving personal data on the websites	54
Figure 20 Percentage of respondents who are using security controls at home	57
Figure 21 Percentage of respondents who answered 'Always' to the above statements (at home) ..	59
Figure 22 Percentage of respondents who answered 'Never' to the above statements (at home) ...	59
Figure 23 Respondents who attended training and their awareness level	60
Figure 24 Percentage for who respondents (received training) think is responsible for information security tasks	61
Figure 25 Families of learning styles (Coffield <i>et al.</i> , 2004a)	83
Figure 26 A map showing the links between personalised learning, individualised learning and different approaches	91
Figure 27 Individual model	102
Figure 28 Group model	103
Figure 29 Collaborative model	103
Figure 30 PLE Prototype incorporating learning styles conceptual model	105
Figure 31 Structure of personalised learning system - Solomon's Learning styles based	107
Figure 32 Summary of study session	111
Figure 33 Table for VARK database October-December 2011: Distribution of preferences	126
Figure 34 ADDIE processes	143
Figure 35 Proposed PISE framework	144
Figure 36 Proposed PISE framework continue	145
Figure 37 Flowchart symbols	150
Figure 38 The Registration flowcharts for Private Trainee	153
Figure 39 Flowcharts for Private trainee	154

Figure 40 Flowcharts for PISE System Administrator	156
Figure 41 Flowcharts for PISE System Administrator (Private PISE)	157
Figure 42 Flowcharts for Private PISE Training Course Administrator	158
Figure 43 Flowcharts for Registration Public PISE Trainee	161
Figure 44 Flowcharts for Public Trainee	163
Figure 45 Flowcharts for PISE System Administrator (Public PISE).....	164
Figure 46 Flowcharts for Public PISE Training Course Administrator.....	166
Figure 47 Screenshot for Private Trainee Registration	169
Figure 48 Screenshot for Public Trainee Registration	169
Figure 49 Screenshot for the Private and Public trainee taking pre-test.....	170
Figure 50 Screenshot for Public and Private trainee view results.....	171
Figure 51 Screenshot for Public and Private trainee view results (continue).....	171
Figure 52 Screenshot for Public and Private trainee learning materials (Visual mode)	172
Figure 53 Screenshot for Public and Private Trainee download modules	173
Figure 54 Screenshot for Public and Private Trainee choose assessments.....	174
Figure 55 Screenshot for Public Trainee Upload modules.....	174
Figure 56 Screenshot for PISE System Administrator dashboard	175
Figure 57 Screenshot for PISE System Administrator Approval	176
Figure 58 Screenshot for PISE System Administrator to assign role to Public trainee	177
Figure 59 Screenshot for PISE System Administrator assign role to Private PISE trainee	177
Figure 60 Screenshot for PISE System Administrator Manage trainee	178
Figure 61 Screenshot for PISE Private Training Course Administrator assign module	179
Figure 62 Screenshot for Public PISE Training Course Administrator updates module	180
Figure 63 Screenshot for Public PISE Training Course Administrator verify assessments	180

List of Tables

Table 1 Classification of information security awareness mechanisms	9
Table 2 Comparisons of information security awareness programme at Aetna and University of Missouri.....	13
Table 3 Respondents by their organisation's industry	30
Table 4 Respondents by their understanding of information security terms	37
Table 5 Percentage of respondents by training location	41
Table 6 Security topics being taught in information security training	42
Table 7 Respondents by sources of information security knowledge at their workplace	45
Table 8 Respondents by sources of information security knowledge at home	51
Table 9 Respondents by their personal information that made visible in social networking websites	55
Table 10 Respondents who said 'absolutely insecure' to put details of personal information on their social networking websites.....	56
Table 11 Respondents by training type and size of organisation.....	62
Table 12 Respondents who understand the below security terms.....	63
Table 13 Respondents by their good information security practices (based in who answered 'Always' at workplace and home).....	65
Table 14 Respondents by their negative security practices (based on who answered 'Never' at workplace and home).....	68
Table 15 Respondents by their good information security practices at home (based on who answered 'Always')	69
Table 16 Comparison of respondents by their opinion about giving personal data on websites	70
Table 17 Comparison of respondents who backup their data on personal computer at home	70
Table 18 Comparison of respondents who answered 'Yes' to the below security controls at home..	71
Table 19 Comparison of sources of information security knowledge between workplace and home	74
Table 20 Comparison of the top three sources of information security knowledge at workplace and home	75
Table 21 Learning styles in adult education.....	84
Table 22 Time taken to complete the experiment.....	116
Table 23 Preliminary study: Comparisons of the pre and post-test results.....	116
Table 24 Participants' information	119
Table 25 The materials used in the study	120
Table 26 Time taken by participants to complete the second preliminary study.....	120
Table 27 Results for the second preliminary study	121
Table 28 VARK classifications and gender	125
Table 29 Detailed scores for Aural participants	127
Table 30 Detailed scores of uni-modal Read/write participants	128
Table 31 Detailed scores of uni-modal Kinaesthetic participant	129
Table 32 Detailed scores of bi-modal participants	129
Table 33 Detailed scores of tri-modal participants	130
Table 34 Detailed scores of quad-modal participants	130
Table 35 Detailed scores of a dyslexic participant.....	132
Table 36 Analysis of the participants' VARK and the Improvement Scores.....	134
Table 37 Detailed scores for participants who scored the highest VARK and highest improvement scores.....	135

Table 38 Detailed scores for participants who scored the second highest VARK and highest improvement scores.....	136
Table 39 Detailed score for participants scored lowest VARK and lowest improvement scores	137
Table 40 Detailed score for participants who has only positive improvement scores	137
Table 41 Detailed scores of participants with mismatched learning style	138
Table 42 Summary of users' roles for Private PISE System.....	151
Table 43 Summary of users' roles for Public PISE System	160

Abbreviations

(ISC) ²)	International Information Systems Security Certification Consortium Incorporation
2HH	2 nd Highest VARK score and Highest Improvement Score
A	Aural
ADDIE	Analysis, Design, Development, Implementation and Evaluation
AK	Aural and Kinaesthetic
A-IS	Aural Improvement score
ANS	American National Standards
AR	Aural and Read/write
ARK	Aural, Read/write and Kinaesthetic
APWG	Anti-Phishing Working Group
BBC	British Broadcasting Corporation
BCS	British Computer Society
BERR	Department for Business, Enterprise and Regulatory Reform
CBK	Common Body of Knowledge
CBT	Computer Based Training
CDSM	Collaborative Skills for Student Model
CERT	Computer Emergency Response Team
CISSP	Certified Information Systems Security Professional
CSCAN	Centre for Security, Communications and Network Research
ENISA	European Network and Information Security Agency
GBP	Great Britain Pounds
GPA	Grade Point Average
GRSLSS	Grasha-Reichman Student Learning Style Scale
HH	Highest VARK score and Highest Improvement Score
IATS	Information and Access Technology Services

IBM	International Business Machines
ICT	Information Communications Technology
IDS	Intrusion Detection Systems
IE	Internet Explorer
IS	Information Systems
ISD	Instructional Systems Development
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ISP	Internet Service Providers
ISPP	Information Security Policy and Practices
ITQ	Information Technology user Qualifications
K	Kinaesthetic
K-IS	Kinaesthetic Improvement score
LL	Lowest VARK score and Lowest Improvement Score
OCR	Oxford, Cambridge, and Royal Society of Arts Examinations
PC	Personal Computer
PISE	Personalised Information Security Education
PLE	Personalised Learning Environment
PLP	Personalised Learning Plan
PSA	PISE System Administrator
MCQ	Multiple Choice Questions
NCSA	National Cyber Security Alliance
NIST	National Institute of Standards and Technology
R-IS	Reading/writing Improvement score
R	Read/write
RK	Read/write and Kinaesthetic
SANS	System Administration, Networking, and Security Institute

SES	Socioeconomic Status
SME	Small Medium Enterprise
SSL	Secure Socket Layers
UCLAN	University of Central Lancashire
UK	United Kingdom
V	Visual
VA	Visual and Aural
VAK	Visual, Aural and Kinaesthetic
VAKT	Visual, Auditory, Kinaesthetic and Tactile
VAR	Visual, Aural and Read/write
VARK	Visual, Aural, Reading/writing and Kinaesthetic
V-IS	Visual Improvement score
VR	Visual and Read/write
VRK	Visual, Read/write and Kinaesthetic

Acknowledgement

This research has been made possible by the scholarship awarded to me by the Ministry of Higher Education, Malaysia through my employer, the International Islamic University Malaysia, for which I am very grateful.

My sincere gratitude to my Director of Studies, Associate Professor Dr Nathan Luke Clarke for his endless support and guidance throughout this amazing journey. Without his excellent scientific knowledge, encouragement and enthusiasm, this work would not have been possible. Very deep and special thanks also go to my other supervisor, Professor Steven Furnell for his insights and great help in this journey. Moreover, I would like to thank to everybody in the Centre for Security, Communications and Network Research Group for their support.

I dedicate this thesis to my deceased mother, Rashimah Mansor, who was indeed a great mother and nothing could replace her in this world. My dedication goes to my dearest father, Talib Rashid, for always being there whenever I needed.

My heartfelt thanks to my dear husband, Muhamad Za'im Ab Wahab, for his love and emotional support. Without infinite encouragement, understanding, support and the baby-sitting service during my final year, everything would have been much harder. Furthermore, I want to thank my dear son, Qayyiem Uqail, for reminding me of what is really important in life.

My sincerest thanks are due to my siblings, relatives, friends and others who have been very understanding and helpful in this PhD journey.

Above all, I give honour and praise to the Almighty God for giving me strength and His guidance throughout my studies.

Authors Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee.

This study was financed with the aid of a studentship from Plymouth University and the full scholarship from The Ministry of Higher Education, Malaysia.

Relevant scientific seminars and conferences were regularly attended at which work was often presented; external institutions were visited for consultation purposes and several papers prepared for publication.

Word count of main body of thesis: 38,298 words

Signed:  _____

Date: 31st January 2014

1 Introduction

Information technology changes the way people perform daily activities, such as online banking, shopping, learning and social networking (Spector and Teja, 2001; Almeida, 2012). Technology has enabled people to share and transfer their personal information via the Internet. These activities have raised the concern as to the security of the information being transferred, especially when it involves personal details such as real name, credit card details and bank account details.

People have become victims of cybercrime nowadays (Hargreaves and Prince, 2013). Indeed, a million adults have been reported become cybercrime victim every day (Symantec, 2011). Statistics from the Cyber Crime Watch online magazine reported that 75 million scams emails were sent every day and affected about two thousands victims (Cyber Crime Watch, 2011). Cybercrime problems have created an annual loss to businesses ranging from billions to nearly \$1 trillion. Hence, making people aware of the importance of information security is very essential as one of the precaution steps to reduce the risk of becoming a cybercrime victim.

Social networking has become a popular trend for making friends (Hunter, 2008; Cook *et al.*, 2011). In these websites, people are able to share their personal information to the public. Here, too, people need to be more educated in terms of privacy issues and more careful when sharing their data.

For many years, information security issues were seen as a technical problem, rather than a people problem (Al-Hamdani, 2006). However, security researchers have realised that technology alone cannot solve the security problem, and it is also caused by a human

problems (Bojanc *et al.*, 2012). Human nature has a tendency to make errors and mistakes (Thomson and van Niekerk, 2012).

Security researchers have thus come to realise that security problems are rooted in human mistakes (Williams, 2008; Lacey, 2010; Mahabi, 2010; El-Haddadeh *et al.*, 2012). Now the security problem is addressed as a people problem, rather than solely on the technical issues.

People need to be educated with information security so that they can protect themselves from these security threats. Therefore, information security education has become very important, as it is recognised as one of the ways to improve awareness and practices. In relation to this, information security awareness and practices play important roles as one of the media for disseminating information on how to protect information assets (Wilson and Hash, 2003).

Organisations have invested in information security training, but there is little evidence that organisations are maintaining the knowledge of their employees. Hence, employees have the tendency to forget what they have learnt in their previous training.

When people attend training, this shows improvements in their security awareness (Schultz, 2004). However, people still become victims of information security incidents as a result of on-going threats (Luo *et al.*, 2011); moreover, they do not practice what they have learnt in the training (Furnell and Thomson, 2009). As such, further efforts to address the issue are warranted.

1.1 Aim and objectives

The aims of the study are to investigate the issues surrounding effective information security awareness, and proceed to propose a novel framework to improve upon the current state of the art.

In order to achieve these aims, the following objectives should be addressed:

- a) understand the current information security awareness and practice domain;
- b) from the prior literature, understand the issues that surround effective information security awareness;
- c) investigate the information security awareness level of individuals within organisations and home environments;
- d) understand how individuals learn within information security training and education;
- e) investigate models of learning and determine the role that learning styles have within education;
- f) to provide an empirical basis for understanding the relationship between learning styles and information security education;
- g) to propose and define a novel framework for personalised learning in security education.

1.2 Thesis structure

The thesis is comprised of seven chapters. Following this introduction, Chapter 2 discusses the state-of-the-art of information security awareness and practices. In this chapter, the current problems and issues in security awareness are presented.

Having taken on board the theoretical issues surrounding effective information security education, Chapter 3 is dedicated to investigating at first hand what information security

awareness is for individuals. Moreover, the survey seeks to better understand how individuals learn and where they learn.

Chapter 4 discusses the further area of learning theories and how people learn differently. In relation to these, here, personalised learning and learning styles are introduced. The chapter also presents the field of pedagogy, and has drawn upon its implementation within secondary education in particular, to better understand its application in practice.

Having understood the requirements for effective information security education and developed a basis for understanding how personalised learning can be achieved, Chapter 5 presents a study into the application of personalised learning in information security. Results of an empirical study are presented that justifies a mixed learning approach to education can be more effective than traditional approaches.

Building upon the study discussed in chapter 5, chapter 6 uses the results to inform a Personalised Information Security Education (PISE) framework. A conceptual realisation of the principles established in chapter 5 is that enables personalised learning within information security. The chapter is split into two sections. The first details the theoretical module and describes the key processes required to develop a personalised learning system. The second section presents a practical manifestation of the model and gives consideration to the practical aspects such a system would introduce.

The final chapter presents the main conclusions derived from this research, highlighting the key achievements, limitations and future direction of the research. This thesis also provides appendices in supporting the discussions in the previous chapters.

2 A Review of Information Security Awareness and Practices

2.1 Introduction

Khan *et al.* (2011) defined information security awareness as ensuring all employees are aware of the organisation's rules and regulations. Kruger and Kearney (2006) refer to the term as a state of knowledge where information systems users perceive, and are aware of the potentially negative impacts of malicious information technology upon their organisation. Wolf *et al.* (2011) have highlighted the need for a clear definition of information security awareness, and suggest the new definition as "the effort to impart knowledge of or about factors in information security to the degree that it influences users' behaviour to conform to policy". NIST viewed the information security awareness as "efforts that are designed to change behaviour or reinforce good security practices" objective as to spread information that relates to information security, to individuals (NIST, 2003). Therefore, information security awareness may be defined as an initiative to improve people's behaviour toward information security practices by disseminating knowledge related to the area.

2.2 The importance of information security awareness

Information security is about ensuring that the confidentiality, integrity and availability of information is not compromised (Pfleeger, 1997; Krutz and Vines, 2007). Confidentiality means that the information should only be accessed by authorised personnel. Integrity is about ensuring that only an authorised person can make changes or delete sensitive information. Availability is about ensuring the information is available for the authorised user when required (Conklin *et al.*, 2005).

Computer technology has influenced the way people perform their daily operations. People have become more dependent upon computers as more processes are computerised and provided online (Turn, 1986; von Solms, 2006).

Chapter 2 – Information Security Awareness and Practices

For example, users are keen to shop online because it is convenient and quicker. They do not have to physically be in a shop and queue at the till to pay their goods (Auta, 2010). Furthermore, some of the virtual shops like Amazon.co.uk offer other incentives such as cheaper prices if you buy online (Amazon.com, 2012). Online banking is another example of such a change. A total of 423.5 million people have used online banking globally in April 2012 (comScore MMX, 2012). Internet banking has become popular because it is more convenient for individuals as it enables them to perform transactions regardless of their location (Auta, 2010). The rapid uptake of various online facilities has led to the need for information security (Graham, 2010).

As more applications and systems have gone online, many of which frequently involve sensitive information being transferred over the Internet, users have become more exposed to Internet threats. A survey conducted by Symantec and National Cyber Security Alliance (NCSA), (2010) shows that 70% of home users were sharing their photos, 68% were shopping online, 65% were using the online banking, and 63% were social networking on the Internet. This portion shows that a significant amount of the respondents are transferring their personal information across the Internet. Thus, it indicates that people need to protect their information while transmitting it over the Internet.

The advent of broadband technology with affordable service packages and unlimited access to the Internet has encouraged people to access to the Internet every keep their computer connected to the Internet all the time (Spurge and Almond, 2003). Connecting to the Internet without essential protection such as updated antivirus and firewall software being installed on the computer will leave people vulnerable to a myriad of information security threats. This has been supported by a survey by Symantec (2007), which illustrated that 95% of targeted attacks are to home users. From the above discussion, the information security is essential in order to protect people's personal and sensitive data.

Chapter 2 – Information Security Awareness and Practices

Mobile technology, such as mobile phone, laptop and Personal Digital Assistant (PDA) have enabled people to be connected to the Internet anywhere they want (Jones, 2008; Smith, 2012). Affordable unlimited package offers by Internet Service Providers (ISP) of the Internet access for mobile devices has encourage people to have their devices connected to the Internet for 24/7 (Quayle and Taylor, 2002; Rangaswamy and Cutrell, 2012; Thomas and Carvalho, 2012). In addition to that, wireless services enable users to be connected to the Internet all the time (Jain *et al.*, 2012). This has made people more exposed to the Internet threats as they keep connected to the Internet services (Toan-Think *et al.*, 2012).

Apart from the above discussion regarding the importance of information security, there are issues in relation to the particular area. According to Tryfonas, Kiountouzis and Poulymenakou (2001), information security issues could be classified into three layers: strategic, tactical and operations. The authors have categorised these issues according to different levels of organisational structure in a company. First, strategic layers comprise of the creation and usage of security policies. Second, tactical is about methods and techniques such as compliance with information security standards, risk analysis conduct, copyright protection and performance of information system audit. The operations are issues regarding tools and product or services features. These include applied cryptography solutions, network security and the use of firewalls, access control mechanisms, software security practises and intrusion detection techniques. These issues are applied to organisations, and emphasised on the different management levels when dealing with the information security. Integrated approach within these three layers of classification should be used to solve information security issues (White, 2009).

However, other researchers have divided information security issues into two; technical and non-technical (Kritzinger and Smith, 2008).

According to them, technical issues are firewalls, intrusion detection, encryption, password protection and access control. Technical issues are dealing with hardware and software to protect the information. While non-technical issues are security policies, legal aspects, ethics, password protection and information security culture. Non-technical issues are more focused on controlling the user or human factors. Based on the information above, information security issues should be taken care of from both a technical and non-technical approach (Inglesant and Sasse, 2011).

2.3 Information security awareness

People have been frequently considered as the weakest link (Whitman and Mattord, 2005; Boss *et al.*, 2009; Al-Omari *et al.*, 2012; Thomson and van Niekerk, 2012). Furthermore, Human behaviours were found contributing to information security breaches (Adams and Sasse, 1999; Besnard and Arief, 2004; Maxion and Reeder, 2005) Thus, there is a need for information security awareness and training especially to those who are dealing with sensitive information. (Wilson and Hash, 2003). Moreover, Power & Forte (2006) has highlighted that information security is a people problem and not a technical problem. This has been supported by Chen, Medlin & Shaw (2008), who believe that security awareness is more important than the technology factor in contributing to success in information security.

Wood (1995) has defined information security awareness as being aware on technology solutions for information security. Previously, information security was considered as more of a technical issue rather than a human issue (von Solms, 2006; Mann, 2008). Siponen (2000) has a different definition about the information security awareness that is, 'a state where users in an organisation are aware of their security mission (often expressed in end-user security guidelines)'.

Chapter 2 – Information Security Awareness and Practices

Wilson and Hash (2003) view the information security awareness as efforts designed to change human behaviour or reinforce good security practices. In the same paper, the researchers have highlighted the differences between awareness and training; 'training seeks to teach skills that allow a person to perform a specific function while awareness seeks to focus an individual's attention on an issue or set'. Wood, (1995); Cone et al., (2007); ENISA, (2007); Hawkins, Yen & Chou, (2000) and Spurling, (1995) have suggested various methods to increase information security awareness. These methods and mechanisms are summarised in Table 1 below:

Table 1 Classification of information security awareness mechanisms

Information security awareness methods	
Reading Materials	Posters, policy, Internet sites, handbooks and guidance, newsletters, desk to desk alerts, memo and circulations, agency wide email messages, subscribing to computer publications
Event based	IT security day, brown bag seminars, awards programmes, face-to-face training, induction training, audit processes, tests and quizzes, crosswords puzzles, automated questionnaires (self-assessed), demonstration of life hacking,
Video based	Videotapes, web-based session/web casting/webinar, teleconferencing, computer based training (CBT), video game, kiosk,
Messages of awareness tools (Trinkets)	Pens, key fobs, post-it-notes, notepads, first aid kits, clean up kits, diskettes with messages, bookmarks, Frisbees, clock, 'gotcha card', pop-up calendar, mascots, stickers, mugs, glass coasters
Hotline	Message machine where information security problems can be reported.
Policy based	Sending warnings if violate organisations' policy, give small prizes or rewards.
Management support	Information security team

Reading materials are security messages that may be either hardcopy or softcopy. Event based are events that give users experience, environment and exposure to current information security issues and threats. Video based are the methods that combined sounds and pictures to make the security message more interesting. Trinkets are one of the creative ways of sending a security message to the user. The message is short, simple and clear to the user. For instance, a security message could be printed in users' post-it-notes as "Do not write your password here". This will give users such a reminder not to write passwords on the post-it-notes.

Policy based mechanism is a method in implementing organisation's policy. It could be sending reminders to those who are breaking the organisation's policy as one of the awareness methods. On the contrary, based on the same mechanism, the management could create a rewards scheme for those who are obey to the organisation's policy. Another mechanism may be in the form of management support. If an organisation has an information security team to support the user, in terms of giving updates and handling users security reports, then the user would be aware of the current security threats and be motivated to report to the team if there is any security incident that had occurred to them. However, implementing security may be very expensive for a company.

Although there are a few methods to increase information security awareness programmes, it is imperative to ensure they are effective programmes (Thompson and Von Solms, 1998; Chen *et al.*, 2008). There are a several methods that have been suggested towards creating an effective awareness programme (May (2008):

- a) Make it personal – create a security message that could be related with people's personal life. For instance, by demonstrating unprotected home computer could be vulnerable to the identity theft threats. When the audience could see the live demonstration, they can remember it easily as compared to just listening to a normal presentation.

- b) Match the message to the audience – create security awareness presentation based on the target audiences. For example if the audience are technically competent, then it is prudent to include the technical jargons in the materials. If the materials are not matched with the audience, the presentation would be less effective.

- c) Keep it short – audience cannot absorb vast amount of information at one time. If the security message could be kept short and simple, then it is easier for them to understand and get the message.
- d) Make it interesting – include some humour in the presentation or reading materials that will catch the readers' attention and motivate them to read more.
- e) Use real life examples – instead of giving theories about security incidents, it is more effective to make the real security incidents as examples and learn from it.
- f) Make it part of everyday business – using posters, short news clips, emails as part of the office decorations and this will make employees conscious about their daily activities that involve information security practises. For example, a poster that reminds user about being aware of people around you before keying in password will make user think and look around before key in their password.
- g) Use the right delivery method – if the audience are IT literate, then using podcasts, online bulletins and other technology based mediums could be a good choice. Nonetheless, using cartoons, colours and images are more suitable for less IT literate.

2.4 Security Awareness

Organisations have become aware that the human being is the weakest link (Schneier, 2000; Gonzalez and Sawicka, 2002), and as such they have been focusing effort, time, money and resources to improve its internal information security awareness programme. They have policies in place to take care of human behaviour in the organisation (Spurling, 1995; BERR, 2008a). Nonetheless, the policy alone is not enough to ensure the employees' awareness in the organisation (Wood, 1997). Indeed, policies have often been referred to as

simply playing “lip service” to the problem for meeting regulations / legislature. Even after reading the policies and knowing their responsibilities with regards to information security, they will still disobey security policy if they disagree with the content of the policy (Schlienger and Teufel, 2003).

There are various measurements and methods to improve information security awareness in an organisation. For example, an international company like DaimlerChrysler has included security awareness as a part of its employees' key performance indicator (Grant, 2007). This indicates that the organisation has viewed user security awareness as a very important issue.

2.4.1. Information Security Awareness at University of Missouri and Aetna

A notable example of a leading awareness programme is at the University of Missouri and Aetna. The goals for the information security awareness programme at the University of Missouri are to change the way its audiences think and act when it comes to information security, to develop metrics to measure the level of the audiences knowledge and the success of the programme, and continually address the importance of information security in the campus environment. The programme has been planned and implemented by the university. Another successful information security awareness programme is conducted by a healthcare benefits company, Aetna. This programme has been awarded as the Information Security Program of the Year Award by Computer Security Institutes in 2002 (Herold, 2005).

Chapter 2 – Information Security Awareness and Practices

Below is the comparison of information security awareness between Aetna (Wright and Kakalik, 2007) and the University of Missouri (McCoy and Fowler, 2004) as shown in Table 2:

Table 2 Comparisons of information security awareness programme at Aetna and University of Missouri

	Aetna	University of Missouri
Types of organisation	Insurance	Education
Security group	Information Security policy and Practices (ISPP)	Information & Access Technology Services (IATS)
Security awareness goals	To persuade all of its users to employ good security practices and behaviours	<ol style="list-style-type: none"> 1) To change the way people think and act when it comes to information security 2) Develop metrics to measure the level of the audiences knowledge and the success of the programme 3) Continually address the importance of information security in the campus environment
Audiences	Employees	<ol style="list-style-type: none"> 1) Students 2) Faculty/Staff
Mechanisms used	<ol style="list-style-type: none"> 1) an intranet security portal, SecurNet 2) an InfoSec newsletter (quarterly published on the SecurNet) 3) barrel pens with security theme with each pen displays one of six possible security messages when the pen is clicked 4) Brown bag lunches (Quarterly) 5) participate in the company's annual Customer Service Fair (using internal events) 6) Posters 7) an InfoSec exam (training and testing annually) 	<ol style="list-style-type: none"> 1) email distribution 2) articles in newsletter (Monthly) 3) advertisement in students' newspaper 4) presentations 5) posters 6) logo and theme (Yearly) 7) In-person training 8) Online training
Limitation	Not specified	Difficulties in defining metrics due to the new implementation of the programme.

Both organisations have adopted security groups in order to carry out information security responsibilities. In terms of security awareness goals, Aetna is aiming to persuade its employees into practising secure behaviours. On the other hand, the University of Missouri is aiming to change the perception of its staff and students towards information security.

2.4.2 Security Awareness for Home users

While organisations protect their systems, some home users are left unprotected and have become the main target for exploitation. According to a survey conducted by Symantec (2007), 95% of all the attacks are targeting home users' sector. Furthermore, a survey stated that attackers are targeting end users instead of computers (Symantec, 2008). This means that traditionally, attackers will launch attacks such as infecting the computers with viruses. Recently, the trends are more towards obtaining end users' personal information such as usernames, passwords and banking details by phishing scams. Once the attackers can access the end users' personal information, they can steal the money from that particular account. According to Phishing Activity Trends Report for the 2nd half 2011, financial services were the most targeted industry sector with 42%, followed by the retail/services 21% and payment services 18%. This shows that motive of many attackers is financial gain (APWG, 2012). Due to these problems, it is necessary for home users to be aware and educated about information security.

According to Furnell et al. (2007), there are a number of reasons that make home users more prone to the computer threats and attacks. Amongst the reasons for this is financial gain. Cases such as online scams are targeting home users who are not even aware of the attacks. While organisations are protecting their systems by having information security policies and procedures, attackers have realised the easier target are in fact home users.

There are challenges to educate home users with information security awareness. Unlike organisation, home users lack the financial resources, the motivation and understanding of the importance such training will provide. If an extra amount of money is required to protect the home systems, then it is difficult for them to implement the security controls in their house.

Home users represent a huge variety of people, from old to young, well-educated to not, disabled and vulnerable individuals and is therefore a far more difficult group to manage and ensure that all of them are receiving information security awareness – whether that be effective or not! For example, home users could be professional workers, school children, universities' students, parents, or the elderly. Professional workers might have exposure in their organisations.

Some schools have taken initiatives to educate their students by taking part in a project conducted by European Network and Information Security Agency (2007) called 'IT Security in primary schools'. The same goes for universities students. Most of universities have an information security policy in place in their institutions (Hawkins *et al.*, 2000). They even have a team of university staff that have specific roles to take care of information security (McCoy and Fowler, 2004). These staff organise programmes such as seminars and campaigns, in an attempt to make students and staff aware of information security. However, this is dependent on the individual whether they choose to join such programmes and embrace information security practises into their daily life. No matter how much effort such educational institutions make, effectiveness still relies upon how the individual embracing the knowledge and applies it within the context of their daily lives. Moreover, the majority of these implemented programmes have little opportunity to understanding how effective such training is.

Whilst school and university students are being educated, parents need to be educated as much as their children. Some parents may learn about the information security in their workplace. Meanwhile, parents not working may learn through self-reading like newspapers and from websites.

For instance, they could learn about how to protect their computer at home from these websites:

- Computer Emergency Response Team (CERT) (CERT Coordination Center Software Engineering Institute Carnegie Mellon University, 2002) – CERT is known as an incident response team, which expanding its role into researching, developing and providing training to improve security The website provides free documents as guidelines for protecting home computers by explaining what should home users do and why it is important to them. The website has listed nine tasks to secure home computers as below:
 - Task 1 – Install and use anti-virus programs
 - Task 2 – Keep your system patched
 - Task 3 – Use care when reading email with attachments
 - Task 4 – Install and use a firewall program
 - Task 5 – Make backups of important files and folders
 - Task 6 – Use strong passwords
 - Task 7 – Use care when downloading and installing programs
 - Task 8 – Install and use a hardware firewall
 - Task 9 – Install and use a file encryption program and access controls
- GetNetWise (GetNetWise, 2008) – This website is a public service provided by the Internet industry corporations and public interest organisations. It is one of the Internet Education Foundation projects aimed to inform public about the usage of the Internet. Through the website, people will be able to read tips and view video tutorials on how to protect their home computers.

Chapter 2 – Information Security Awareness and Practices

- Get Safe Online (GetSafeOnline, 2009) – Get Safe Online is a funded by several UK Governments' departments and private sector businesses. It provides advice and guidance to public on how to protect themselves, computers, mobile devices and businesses against fraud, viruses and other problems encountered online. People will also be able to get news and updates on related issues through the website.
- Internet Safety Zone (Internet Safety Zone, 2012) – the website is provided by Cyberspace Research Unit at the University of Central Lancashire (UCLAN), UK. It offers information on the Internet safety for parents, teenagers, young children under 13s and young adults. The website provides information based on the aforementioned readers' group. For example, the parents section gives information on how to secure themselves and their children, the issues that they need to know and how to report and handle incidents. For teenagers, the website offers information on the dangers of eating disorders, grooming, sexual contents, suicide and violence, cyber bullying, prejudice and discrimination, gaming, social networking sites, email, chat and instant messenger, blogs, mobile phones and browsing. The website also provides information on how to get certified in Internet Child Safety at UCLAN.
- Microsoft (Microsoft, 2009) – The website is provided by Microsoft company. People would be able to download security tips for protecting home computers from viruses, spyware, and other malware. It also provides the latest security updates for windows user, and free antivirus online scanner for public.
- National Cyber Security Alliance (NCSA, 2008) – The website is named Stay Safe Online.org. Developed and maintained by NCSA. It provides information on how be safe when online and giving opportunity to public take part in the information security awareness initiatives such as supports the information security awareness month by conducting it in their own organisation. The website provides free resources to promote the awareness. For example, people would be able to download posters, templates. Letterhead and web banners.

- For business person, they would be able to download resources related to secure their business and view security videos via the website. Like Internet Safety Zone, the website also provides information security tips and advices for parents, teenagers and public community.
- The Sans Institute (SANS, 2008) – The website is provided by the Sans Institute. It provides a section called SANS InfoSec Reading Room where people would be able to download and read free white papers regarding home and small office. The readers may also view the free webcasts by knowledgeable speakers from the website resources.
- WebWise (WebWise, 2012) - The website is provided by the British Broadcasting Corporation (BBC). People would be able to read basic information on the online safety and privacy from the website. It also provides other information on how to use computer, web browsing and social networking. People are able to learn short courses on using mobiles, using email, using the Internet, and safety activities. The courses are free, and people may pay money to be certified as IT user Qualifications (ITQ) awarded by UK recognised body such as; British Computer Society (BCS), City & Guilds, and Oxford, Cambridge and Royal Society of Arts (RSA) examinations (OCR).
- WiredSafety.org (Wired Safety, 2012) – Wired Safety is provided by volunteers from range age of 7 to 96 who are TV personalities, teachers, law enforcement officers, PhD's, writers, executives, librarians, stay-at-home moms, retired persons, Walmarts' greeters and students. The resources from the web page are free of charge except TeenAngels, outreach, law enforcement training, and speaking programs. People are able to find resources as below:
 - a) Help and support for victim of cybercrime and harassment
 - b) Advice, training, and help for law enforcement worldwide on preventing, spotting and investigating cybercrimes

- c) Education for children, parents, communities, law enforcement and educators
- d) Information and awareness on all aspects of online safety, privacy, responsible use and security
- e) Resources that can be downloaded or printed and used for offline presentations, community events and classroom activities

However, a question arises regarding how people learn about information security. Furthermore, even though these websites provides guidance and advice, the main concern is how to motivate and attract parents to go to these websites and read the materials in the first place. Some of them are not aware of the existence of these websites especially if they are novice users (Kritzinger and von Solms, 2010). Even though if they are aware of the websites they probably do not know which level of information security that are relevant to their level of knowledge (Kritzinger and von Solms, 2010). From the above examples of free resources on information security awareness, two of them (Internet Safety Zone and WebWise) provide an opportunity to get certified with their free courses as one of the ways of motivating people to learn about information security. However, it is possible that some of the parents who have an interest in security might read the materials and teach themselves.

Since almost all age groups have been discussed earlier, the only one left is elderly people. According to Cook *et al.*, (2011) the weaknesses of the current information security portals and websites are not satisfy the need of senior novice computer users. They also suggest that the security portal should improve the inefficiencies in terms of conduits of language, accessibility and hypermedia that are suitable to the age group. Little research has been done on the awareness initiatives for this elderly group.

2.5 Conclusion

As referred to in the previous discussions about effective information security awareness programmes, one of the suggestions is to match the security programme to the audience (Thompson and Von Solms, 1998; May, 2008). Information security awareness is important, regardless of being an employee or home users. This is because the nature of daily activities is changing, and there are information security threats that could harm people. Previous information security initiatives are one size fits all and this need to be improved to raise people's awareness. In addition to that, the learning materials on the information security are not created based on people's learning preferences such as learning styles. People may learn about information security via the websites listed in the previous section and be certified if they are interested to expand their knowledge to the next level. Current levels of people's awareness on information security need to be assessed in order to improve this level of awareness. Therefore, a survey on information security awareness has been conducted, in order to explore the awareness level amongst people.

3 An Information Security Awareness Survey

A survey on information security awareness is conducted not only to investigate level of awareness but also to find if there is transferability of information security knowledge between the workplace and the home environment. Organisations may provide information security training to their employees so that they understand their roles and perform their task more efficiently (NIST, 2003). These employees might then change their security behaviour not only in the workplace, but also in their home. According to the Decomposed Theory of Planned Behaviour by Taylor and Todd, peers and superiors' influence affected people's perceptions, which leads to their change of behaviours (Taylor and Todd, 1995). In terms of information security practice, it may be assumed that people might have security behaviour influenced by their superiors and colleagues in their workplace, and also their peers at home. Hence, this leads to the idea of transferability of knowledge and practices within organisation and the home environment. In order to investigate the transferability of information security knowledge, a set of data was collected from people who are currently employed in any organisation to participate in this research.

3.1 Purpose of the survey

The purpose of the survey was to investigate the information security awareness level of those who are currently employed in any organisation, in terms of their security practices within the workplace and at home, and how they learned the knowledge. Below are the main objectives of the survey:

- a) to understand/assess the current level of information security awareness among employees in organisations;
- b) to understand/assess sources of information security knowledge;

- c) to understand/assess the current information security practises in workplace and at home;
- d) to identify the transferability of information security knowledge/skills from workplace to home and vice versa;
- e) to assess the effectiveness of information security training on employees' information security practises within the workplace and at home;
- f) to find out what type of training approaches people most preferred

3.2 Research method

This research adopted a quantitative research methodology. As the main objective of this research was to investigate the transferability of knowledge, this method appeared to be the most suitable approach. In addition, a quantitative method was felt to provide a clear answer to the investigation in terms of providing evidence as to the existence of the transferability of knowledge. The technique of data collection carried out in this research was that of the online survey. Online survey provides access to variety of people in a population that is difficult to reach by other channels (i.e. face to face meeting difficult to reach by other channels (Garton *et al.*, 1999). Moreover, this technique had its strength in terms of reaching respondents coming from various locations.

3.3 Methodology of the survey

The survey was conducted online for a period of 49 days (20th August – 7th October 2008). The survey was targeted to receive at least 300 participants, and this explained why the survey was stopped after 49 days. The questionnaire was approved by the Faculty of Technology Ethics Committee before it was made available online to the public. This was to ensure that the survey would observe the university's ethical principles for research involving human participants.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

The approval form for the ethic's approval is attached in Appendix A. Respondents of the survey were selected based on the researcher's academic contacts, personal contacts and from the word-of-mouth. The link for the survey was also disseminated using email and some mailing lists such as Google and Yahoo groups.

The survey was designed to answer the following questions:

- a) What proportion of people practice information security in the workplace and at home?
- b) What is the current information security awareness level of the respondents?
- c) What are the sources of information security knowledge of the staff at workplace and home?
- d) Is there any transferability of information security knowledge between the home and the workplace, and vice versa?
- e) Does information security training have any effect on those who have attended it?
- f) What are the preferable types of learning approach for information security awareness programmes?

The survey consisted of 29 questions and was organised into four sections; Section A: Demographics; Section B: Information Security Awareness; Section C: Practises in the Workplace; and Section D: Practises at Home. The copy of the questionnaire is attached in the Appendix B.

Section A (Demographics), was designed to find information about the respondents of the questionnaire. The target respondents were those who were employed, and this explains why the age group started with 16 year old. According to BERR (2008b), the legal age for a person to work full time is 16 years old. The age gap was then divided into 10 years blocks.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Section B (Information Security Awareness), aimed to establish the current information security awareness of respondents. In order to know what respondents think about their level of information security awareness and computing skills, questions 8 and 9 were designed to obtain this information. In order to capture respondents' understanding about information security, question 11 asked about common information security terms. Lists of the security terms were based on a combination of security terms from various sources (CERT Coordination Center Software Engineering Institute Carnegie Mellon University, 2002; The Trustees of Indiana University, 2005; Australian Computer Emergency Response Team, 2008; Kelley, 2008; Network Dictionary. Com, 2008). In addition two additional meaningless or fake security terms (Phlopping and Whooping) were created in order to test the validity of participants' answers to the survey.

Section C (Practices at Workplace) sought to investigate the current practise of respondents in their organisations. Question 12-16 asked about information security training and awareness programmes conducted in the workplace. In order to have more understanding about what kind of security knowledge these respondents learned in their workplace, question 15 was created. The question required respondents to tick which security topics that they had learnt during their training. Lists of topics in question 15 were based on the domains of information security controls in British Standard International Organisation for Standardization (ISO)/International Electrotechnical Commission (IEC) 17799:2000(E) and ISO/IEC 27002:2005. Apart from asking about security training, sources of security knowledge were asked about in the section. Thus, questions 17 and 18 enquired as to the sources of information security knowledge and enabled respondents to rank the top three sources at the respondents' workplace. Question 17 also provided indirect information regarding the transferability of information security knowledge from home to workplace. At the end of the section, 17 statements pertaining to respondents' practices in their workplace were listed.

Section D (Practices at Home) presents the comparisons of current practises in this and the previous sections were used to determine the level of transferability of information security knowledge for the respondents. Question 21 and 22 asked about the sources and rank of information security knowledge at home. In order to understand more about respondents' practises at home, Question 23 was created with the aim of finding out whether respondents were interested in information security and reading about it at home.

Since social networking using websites is quite popular amongst the public, Question 24-26 were created with the aim of finding out information regarding the social networking activities of respondents and their awareness of divulging personal information over the Internet. Question 27 gave information about security application/controls that respondents were using at that time. For a further understanding of security practises at home, Question 28 was designed in a similar way to Question 20, except for a few additional statements to suit the participant's security practises at home. Respondents were finally given the chance to provide suggestions and comments for future improvement of information security awareness training in Question 29.

3.4 Validation of the survey

The first pilot test for the survey has been conducted on 29th April 2008 to an English class for PhD students. The survey was distributed in a hardcopy version. Eight participants tested the survey. Their backgrounds of knowledge were the Arts, Biology, Statistics and Mathematics, Language and Computing. Since the target respondents were not specifically those who were in the computing area, the mixed knowledge backgrounds lent themselves well to the pilot test. This also ensured that other people who were not specifically working in the computing area could understand the questions in the survey. The first version of the survey is attached in the Appendix C at the end of this report.

The participants took about 20 minutes to complete the survey. Overall, the participants were able to understand most of the questions; only a few of them experienced difficulties in answering them. Some respondents had difficulties in answering the questions due to information security jargon such as backup, cryptography and firewall, but after the participant's comments are about jargon, the survey was improved by providing definitions to all information security jargons to enable participants to answer the question accordingly.

The second pilot testing phase was an online version of the survey. There were 11 participants who completed the survey. Six of them were from the Centre for Security, Communications and Network Research (CSCAN), and the remaining five were from different knowledge backgrounds. This time the participant knowledge backgrounds were Medicine, Coastal Engineering, Computing and Arts. Again, this was seen as a good combination of participants in order to ensure that the survey could be understood by people from different backgrounds. For participants from CSCAN, their comments were taken in real-time whilst they undertook the survey. Other participants were asked to test the survey using their personal computer, in their own time. Most of them commented about the length of the survey, preferring it to be shorter and simpler than the tested version. Thus, the total number of questions was reduced from 43 to 29.

3.5 Filtering mechanism

Two fake security terms, Phlopping and Whooping, were created in question 11 as one of the mechanisms to check whether the respondents were answering the questions properly or whether they were simply ticking the check boxes for the security terms. For respondents who answered both terms as "I understand it", these users' responses are closely examined or rejected.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Those who answered “You have heard of it but are not sure what it means” were thought to have misheard the term somewhere, and their responses could be accepted.

The other mechanism was to check the consistency of respondents answering (question 17 and 18) and (question 21 and 22). Below are the questions that were asked of the respondents:

Q17: What is/are the source(s) of your information security knowledge in your workplace?

Q18: Please rank only three (3) of the most useful sources of your information security knowledge in the workplace (Most useful ← 1 2 3 → Least useful)

Q21: What is/are the source(s) of your information security knowledge at home?

Q22: Please rank only three (3) of the most useful sources of information security knowledge at home (Most useful ← 1 2 3 → Least useful)

In question 17 and 21, there were 20 sources of knowledge (including Other) to be selected. Respondents were asked to choose as many sources as they thought would be useful to them. Then, in question 18 and 22, they were asked to rank the top three of their choices in question 17 and 21. An example of the checking process was to check whether all the chosen sources in question 18 should be chosen in question 17. The same process applied to question 21 and 22. This was because if the respondents ranked the sources that they did not choose in question 17 and 21, they were considered as not paying attention when answering questions in this questionnaire. In summary, respondents who answered “I understand it” for both fake terms, and had both inconsistencies with (Q17 and Q18) and (Q21 and Q22), were excluded from the survey analysis.

3.6 Survey findings

The survey received 551 participants (missing fields' responses were included), 339 of which were full respondents (full means there were no missing fields for each respondents), and after filtering using the four mechanisms in the previous section, 333 responses were utilised for the analysis in the survey. A copy of the survey question can be found in the Appendix B and the full results of the survey and responses are attached in Appendix D.

3.6.1 Demographics

The results showed almost an equal split between male and female respondents, with 55% male and 45% female. The majority of the respondents came from two countries, Malaysia and United Kingdom. This was due to the personal contacts of the researcher.

Whilst these countries certainly did not represent a sample of countries globally, the country a respondent was from was not expected to play a significant role in this survey. It would therefore be appropriate to assume the responses made in this survey were representative of people who are currently employed. In terms of the age range; the majority of the respondents were between the ages 25-34, as illustrated in Figure 1.

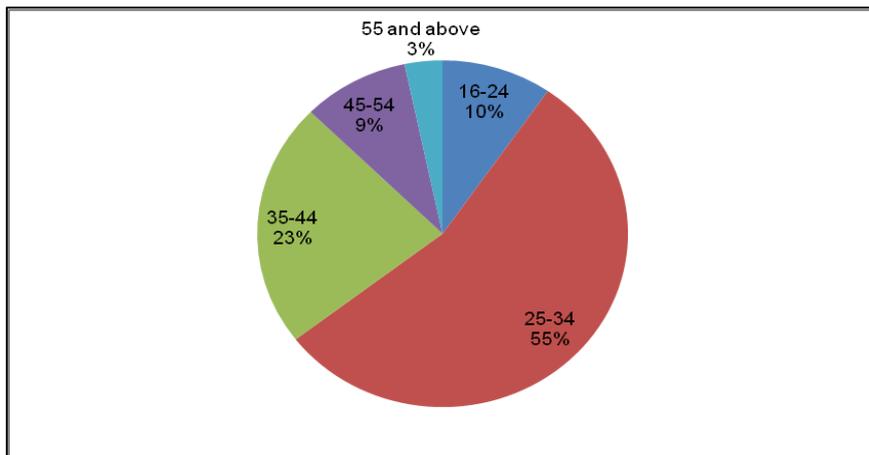


Figure 1 Survey respondents by age range

Chapter 3 – Survey of the Transferability of Information Security Knowledge

When assessing respondent's highest level of education, it was found that 46% of them had the highest level of education as postgraduate, followed by 35% of undergraduate. This was illustrated in Figure 2. This showed that a large portion of the respondents were highly educated. In terms of respondents' organisation's industry, the majority of them were from training and education industry. The breakdown of other industries is given in Table 3.

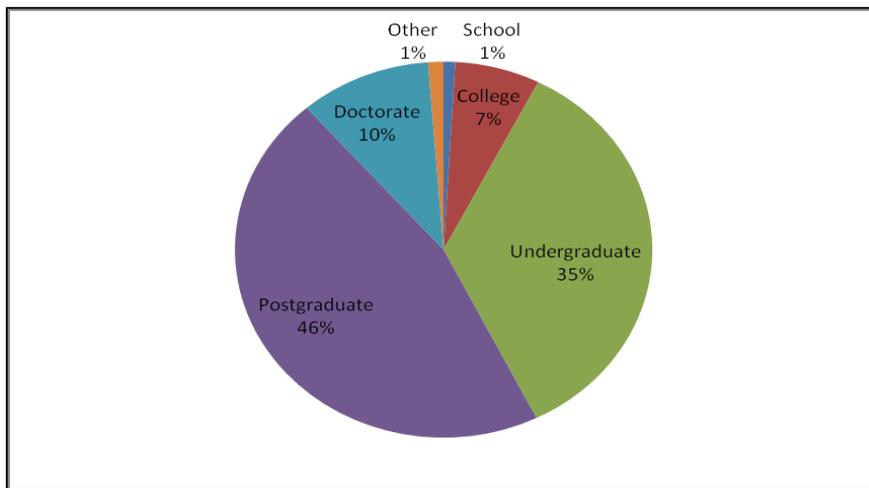


Figure 2 Respondents by their highest level of education

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Table 3 Respondents by their organisation's industry

Industry	No of Respondents
Education/Training	158
Technology	45
Government	25
Telecommunications	21
Other	16
Engineering/Architecture	15
Manufacturing/Operations	8
Healthcare	7
Construction/Facilities	5
Internet/New Media	5
Art/Entertainment/Publishing	4
Accounting/Finance	3
Law Enforcement/Security	3
Pharmaceutical/Biotech	3
Clerical/Administrative	2
Customer Service	2
Management Consulting	2
Advertising/Public Relations	1
Banking/Mortgage	1
Hospitality/Travel	1
Insurance	1
Marketing	1
Military	1
Non-profit	1
Real Estate	1
Transportation/Logistics	1
TOTAL	333

Respondents were also asked about their size of the organisation. The result indicated that a large group of employees (73%) were from large enterprises¹ that had a number of employees, from 251 and above. The remaining 27% were from organisations below 251 employees. This information is depicted in Figure 3.

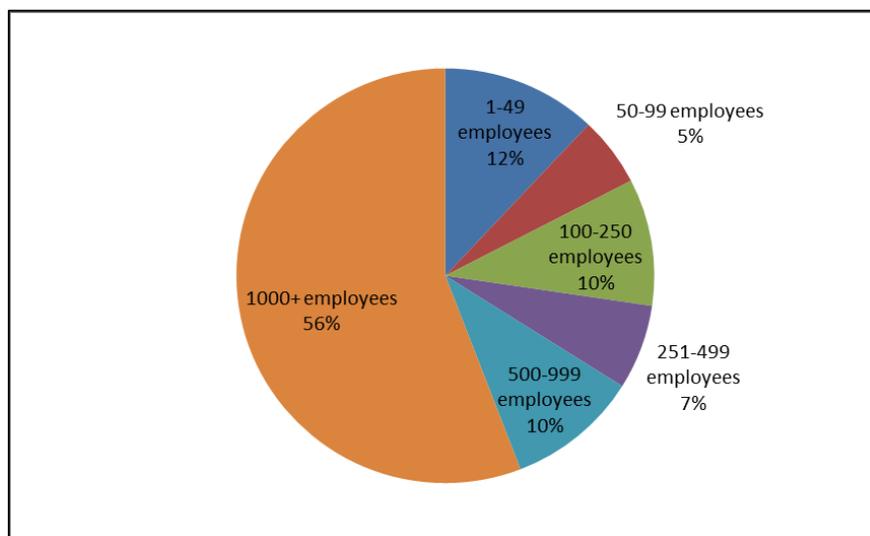


Figure 3 Respondents by their size of organisation

The majority of the respondents were normal employees, accounting for 60% as compared to other roles specified in Figure 4. A total of 15% of them were managers and another 15% were team leader/supervisors.

¹ The definition of large enterprise is based on the definitions given by the Department for Business Enterprise

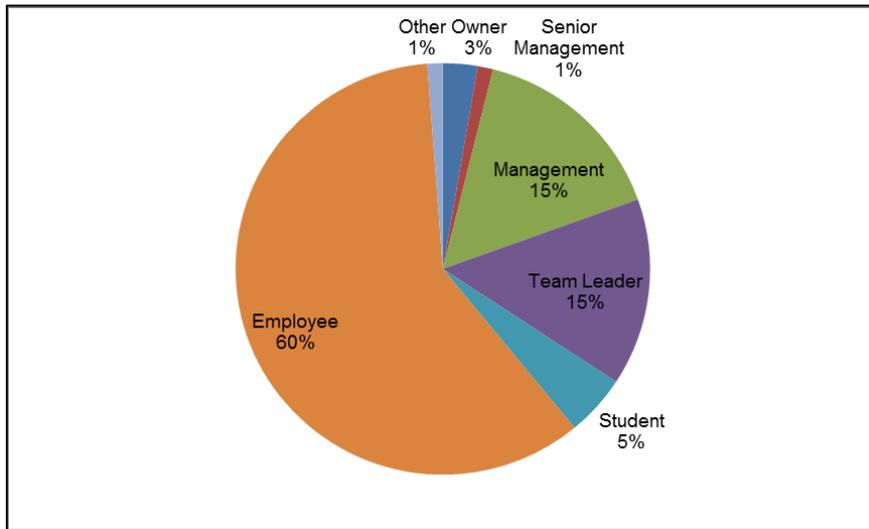


Figure 4 Respondents by their primary role within the organisation

3.6.2 Information security awareness level

The survey was designed in order to find, amongst other things, the current state of peoples' information security awareness. In particular, this survey was interested in people who were currently working in organisations. The respondents were asked to rate their awareness level. This has been illustrated in Figure 5. A total of 34% of the respondents rated themselves as high and 15% as having a very high level of security awareness. 40% of the respondents rated themselves as average, while 7% and 3% rated their awareness level as low and very low level respectively.

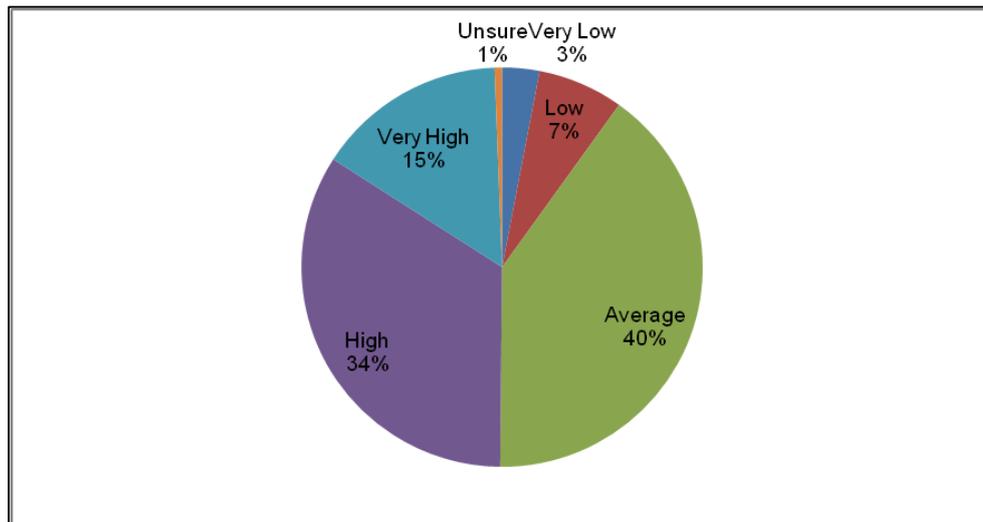


Figure 5 Information security awareness level

In terms of respondents' Internet/computing skills, a large portion of them considered themselves as advanced users. This could be seen from Figure 6, where 44% claimed to be advanced and 20% as experts' users. Since the majority of the respondents rated themselves as advanced and expert/professional computer users, this was one reason why they had such high levels of awareness. In relation to this, Figure 7 also showed that those who rated themselves as having an intermediate level of computing skills were rated average in their level of information security awareness. This result seems to suggest an over-confidence in their rating of their level of awareness.

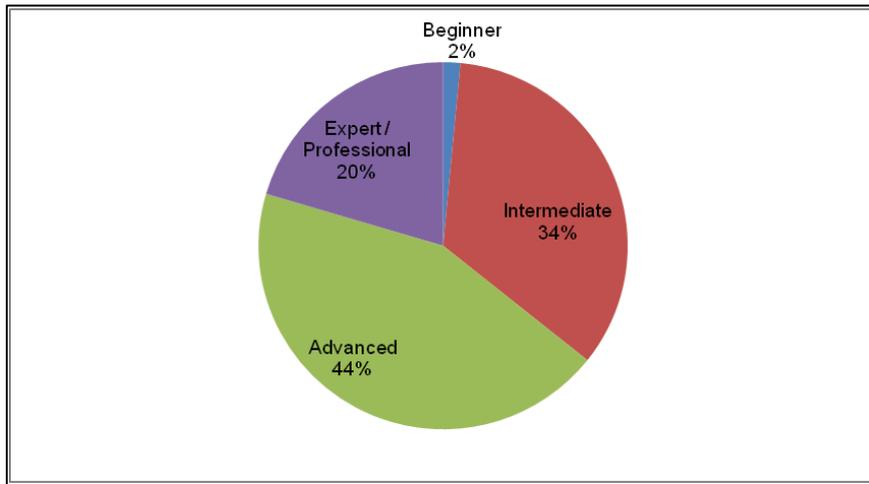


Figure 6 Respondents by their Internet/computing skills

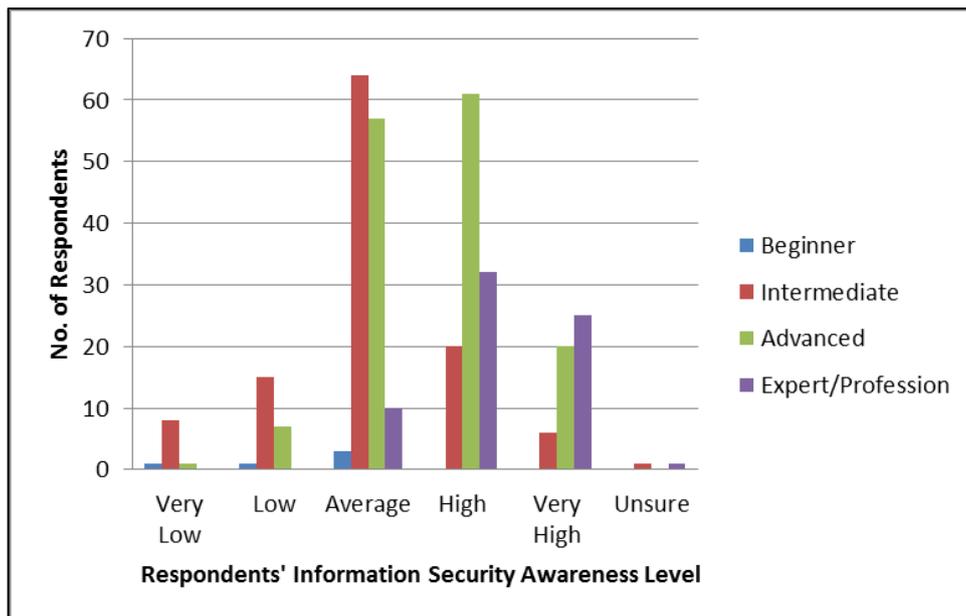


Figure 7 Respondents' information security awareness level and Internet/computing skills

In order to assess respondents' security awareness, the question of who is responsible for the security task has been asked. A total of 70% of the respondents believe that system administrator should be responsible to the security tasks as illustrated in Figure 8. A total of 59% were aware that it was their responsibility as an individual user to protect their computer systems from threats. This illustrates that even though they think that the system

Chapter 3 – Survey of the Transferability of Information Security Knowledge

administrator should be responsible for all the protection, little more than 30% of them understood the idea that information security was everybody's responsibility.

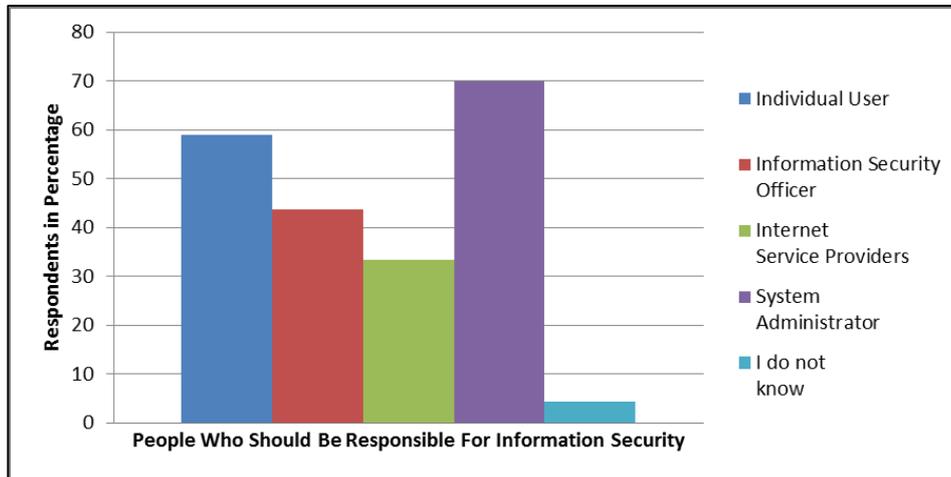


Figure 8 Percentage of total respondents about who they think is responsible for information security tasks

In order to understand the level of the respondents' security awareness, seventeen terms of information security threats were asked to clarify whether the person understood, had heard of it or never come across of the term. Referring to Table 4, three security terms were understood most by the respondents. These were: hackers, virus/worm and spam. This might be due to their common usage in newspapers, magazines and other media. The term virus/worms is used by numerous antivirus software companies and the products are sold on the shelves in various computer shops. This might be another reason why 92% of the respondents were familiar with the term. Since the majority of users were above average in terms of computer skills, they might also have been familiar with the email application. Therefore, it is possible that they had come across the word 'spam'. The term pharming and zero days' attacks turned out to be among the lowest percentage of respondents that understood the security terms (excluding the fake terms). This might be because the two

terms are quite new in the security area as compared to other terms. Social engineering has become a recent trend for the attackers.

This is quite worrying, as only 44% of the respondents were aware of the social engineering attacks. In 2003, phishing attacks were of concern to the public. About 2 million users gave their personal information to bogus websites, and resulting in a \$1.2 billion loss to U.S. banks and credit cards issuers (Litan, 2004). Banking institutions have taken the responsibility to educate all their customers not to fall into the phishers' trap. Five years later, efforts have become fruitful, with 70% of respondents being aware of this threat.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Table 4 Respondents by their understanding of information security terms

Information Security Terms	You understand it (%)	You never heard of it (%)
Virus/Worm	92	0
Trojan horse	80	3
Spam	90	0
Social engineering	44	24
Phishing	70	10
Pharming	24	42
Identity theft	81	8
Key loggers	57	22
*Phlopping	7	68
Botnets	33	43
Zombies	33	38
Denial of service	56	24
Packet sniffer	47	37
*Whooping	10	59
Hacker	95	1
Zero day attacks	29	44
Cracker	56	24

*Fake security terms

Amongst the seventeen terms, two of them were intentionally created as measurements to determine the validity of the respondents' answering the questions. The two terms are "phlopping" and "whooping". Figure 9 and Figure 11 illustrate the cross-analysis between level of security awareness of the respondents and their understanding of these fake terms. Interestingly, respondents who rated themselves as average were better in responding to these two terms, as compared to those who claimed to have a high and very high level of

Chapter 3 – Survey of the Transferability of Information Security Knowledge

awareness. This could be due to the fact that respondents might think that they had an average level of awareness, but their actual level could be high, or very high. The same pattern could be seen between those who rated themselves as high and very high. On the contrary, respondents who claimed to be high and very high could be assumed to have a high level of confidence to consider themselves at those levels. This shows that although the respondents rated themselves as having an above the average level of awareness, this does not mean that they can actually understand the security terms and can be considered as what they claimed to be. The same assumption could be applied for average respondents, where their actual level of security awareness was higher than what they claimed to be.

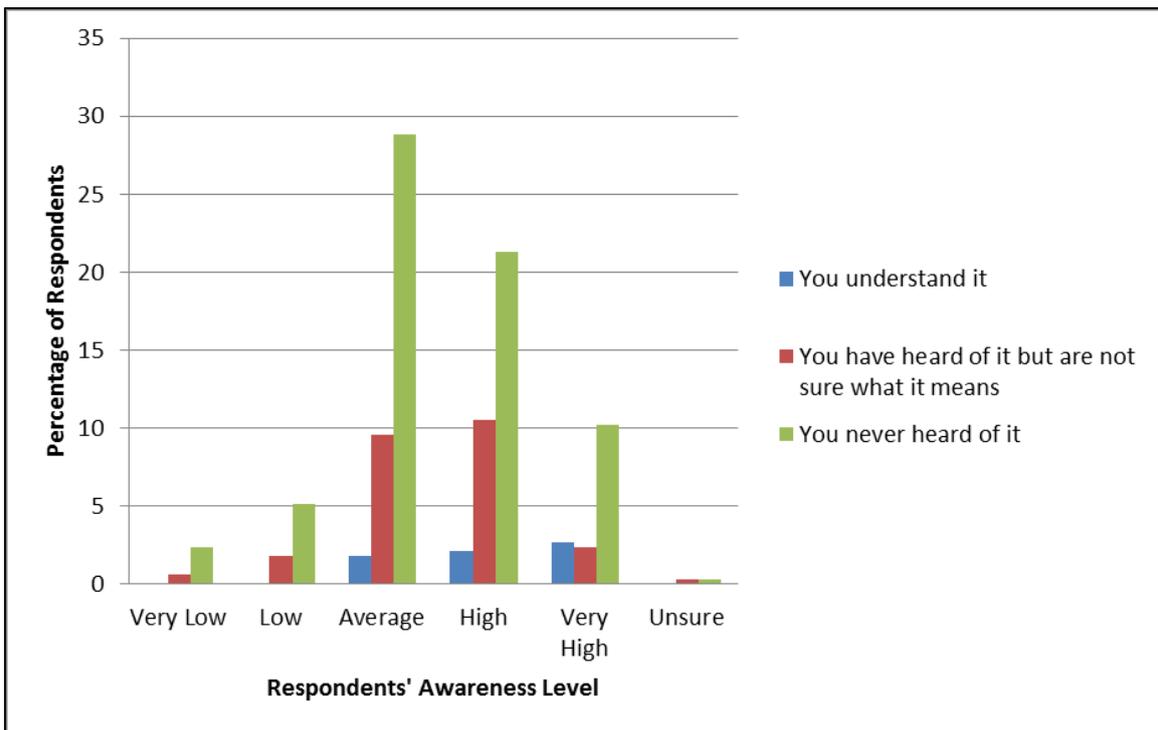


Figure 9 Security term 'Phlopping' and respondents' security awareness level

Chapter 3 – Survey of the Transferability of Information Security Knowledge

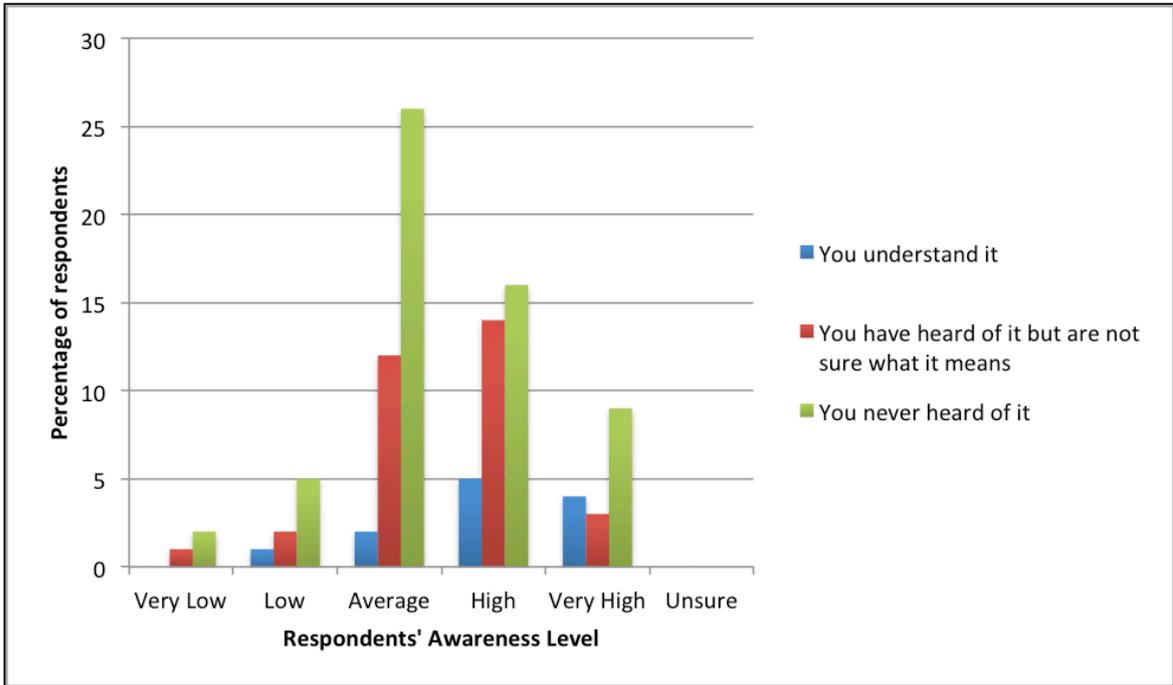


Figure 10 Security term 'Whooping' and respondents' security awareness level (in percentage)

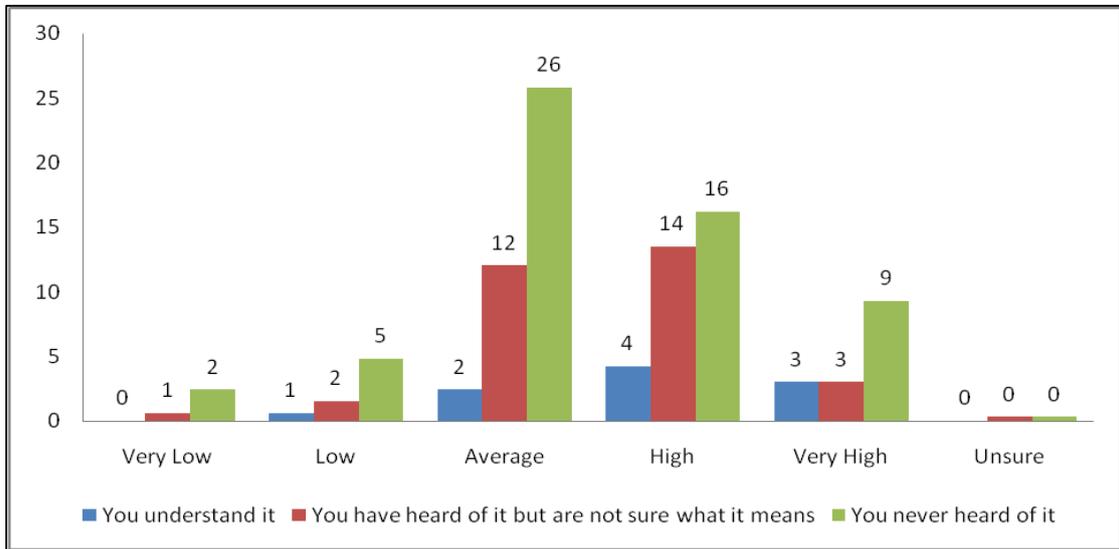


Figure 11 Security term 'Whooping' and respondents' security awareness level (in percentage)

3.6.3 Information security practices at workplace

In the survey, respondents were asked about their security training experiences at their workplace. 36% of them claimed that their organisations provided information security training. The information, as illustrated in Figure 12 shows that organisations do provide security training to their employees. Amongst the 36% of total respondents, 95% of them attended the trainings provided. This is indeed a good sign, with the employees using the opportunity to learn about information security. In the same question, 31% of the respondents stated that they did not know about the training. This shows that there are respondents who are not familiar with the term security awareness and training, so their organisation might have provided such training, but unfortunately, they were not aware of it.

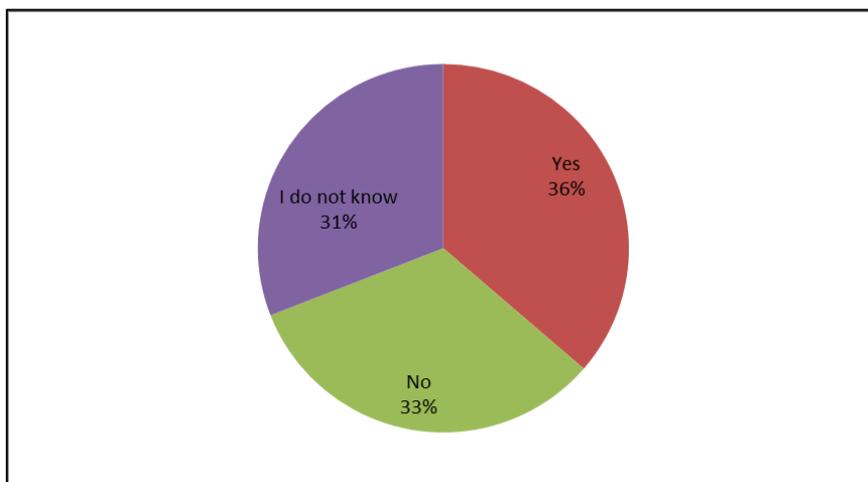


Figure 12 Respondents by information security training provided in their organisation

Apart from asking if the organisations provided training, a question about how frequent the respondents attended training was asked. This is depicted in Figure 13. The majority of them attended on a yearly, monthly and quarterly basis. This could be due to the limited budget and time available in their organisations.

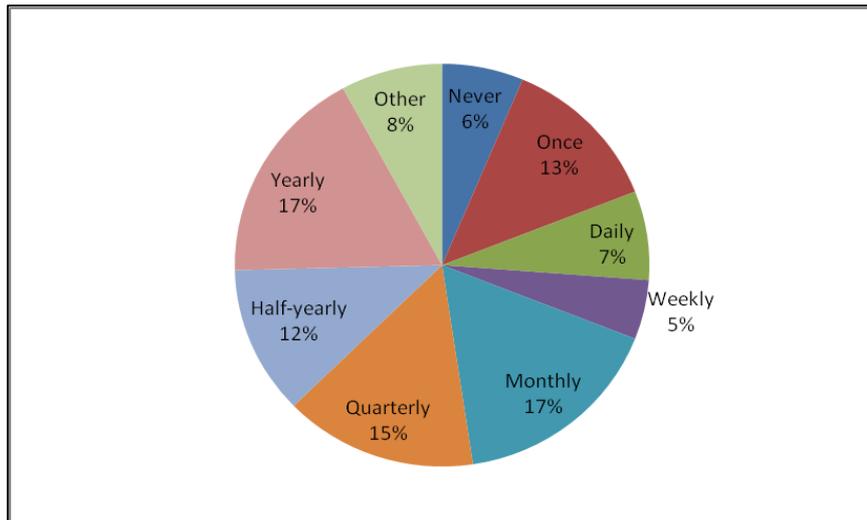


Figure 13 Percentage of respondents by frequency of attending security training

In order to understand more about the training in organisations, a question regarding training location was asked in the survey. Table 5 below demonstrates the percentages relating to how the trainings were been conducted in respondents' organisations. The majority of the organisations supported self-study training. The reason for this may be due to the advantage of self-reading, as the respondents had the flexibility to choose their own time and place to read the training materials and less cost.

Table 5 Percentage of respondents by training location

Training Location	Percentage (%)
In-house by organisation's experts	26
Self-study	28
Outside organisation	16
In-house by outside experts	15
Online training	14
Other	1

Chapter 3 – Survey of the Transferability of Information Security Knowledge

The second highest portion was the training being conducted within the organisation with an internal trainer. This could be due to the costs, whereby it is cheaper to conduct training internally and utilise their own experts. However, there are different costs for the location if the trainer is from the same organisation, or invited trainer from outside. This might explain why only 15% of organisations have invited outside experts, as compared to those organisations that are utilising their internal experts to teach the trainees. Respondents were asked about what kind of security topics were taught in the training that they had attended, the results of which are presented in Table 6 below. Security policy and network security are the most popular topics. This shows that most of the respondents are being exposed about what they should and should not do in the organisation. In addition to this, these respondents could also be considered as at least having a basic idea of how to protect themselves while they are connected to the Internet.

Based on the same table, 92% of the respondents learnt about access control systems in their training. It might be assumed that respondents are aware of passwords, firewalls and authentication processes. Overall, those who attended the trainings could be expected to have an idea, or at least be familiar with information security topics in Table 6.

Table 6 Security topics being taught in information security training

Security Topics	Percentage (%)
Security policy of the organisation	93
Security and risk management	88
Access control systems	92
Network security	93
Secure communication	70
Legal issues	76
Impact of security breaches on the organisation	81
Physical and environmental security issues	80

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Apart from the security topics being taught in the training, respondents were asked about what kind of learning methods that they had experienced. As illustrated in Figure 14, presentation was the most common method experienced by the respondents. The reason for this might be that a presentation is the established method for any kind of training. The second popular training method experienced by the respondents was that of email security alerts. Since email is widely used medium of interaction between employer and its employees, this could be the reason why it was used as a popular training method. Furthermore, using email is faster, has fewer costs and the participant could read in their own time. The third method of training involved is using handbooks and a Web based awareness course. This could be because participants are usually given handbooks in most training programmes.

The reason for web based course being quite popular might be due to the trends of using online training, which will reduce the costs of being present physically in the training place.

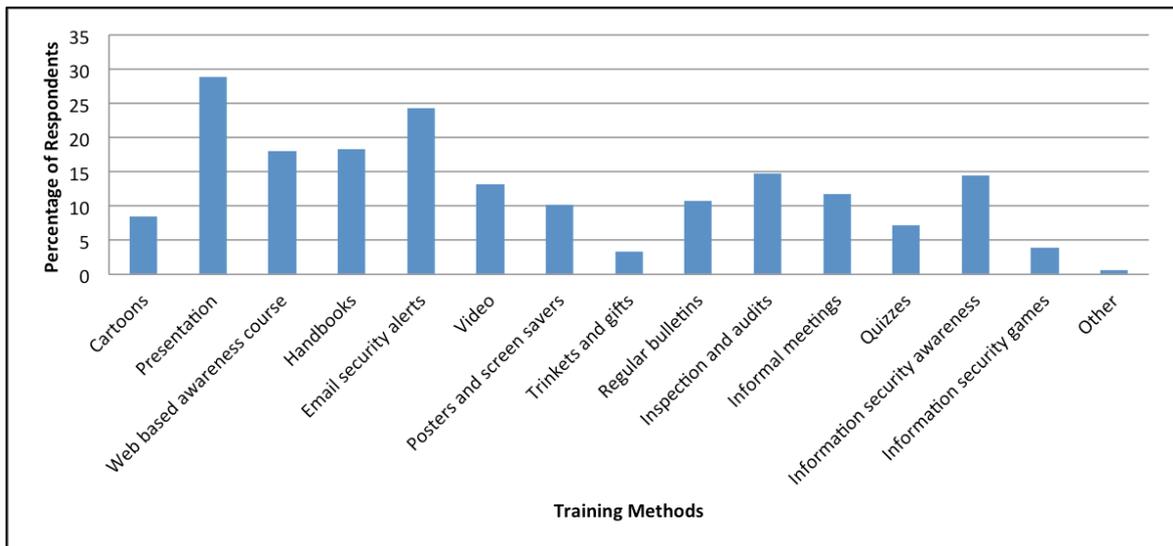


Figure 14 Percentage of respondents by experienced training methods

Chapter 3 – Survey of the Transferability of Information Security Knowledge

One of the objectives for the survey is to determine the sources of information security knowledge at workplace. Based on Table 7, 75% of the total respondents commented that their sources of information security knowledge in the workplace are from websites and using search engines to find the information. One of the factors that might contribute to this is that most organisations are giving their employees' access to the Internet to facilitate their daily operations. In addition to this, it is easier and faster for them to retrieve the information that they need about information security via websites and search engines. 57% of the respondents claimed that their sources of security knowledge came from discussions among themselves and their professional contacts. This demonstrates that there are discussions about information security taking place among the respondents and their colleagues in the workplace. 47% of the respondents said that they had learnt about information security from their organisation's policy. This illustrates that employees do learn from policy documentation.

A further objective of this survey is to determine if there is a flow of knowledge transfer from the workplace to the home and vice versa. From Table 7, 29% of the total respondents claimed that they learnt about information security at home. This indicates that there is a knowledge flow from the home to the workplace. Respondents might have learnt from their family members or friends that stay under the same roof. Another possibility is that respondents might use their leisure time at home to read information related to information security. However, people should be careful in accepting knowledge informally as the accuracy of the information could be questioned.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Table 7 Respondents by sources of information security knowledge at their workplace

Sources of Information Security Knowledge	No. of respondents	Percentage
Websites and search engines	250	75
Information discussions with colleagues, professional contacts	190	57
Organisation's policy	156	47
Books	117	35
Magazines	115	35
Professional activities (conferences, meetings, briefings, etc)	103	31
From what I learnt at home (e.g. family members, friends)	97	29
Academic journals	92	28
Daily Newspaper	91	27
Presentation	90	27
Research articles	80	24
Hearsay	78	23
Pamphlets/brochures	65	20
Government or professional reports	61	18
Posters	51	15
Television news	43	13
Radio	22	7
Interview	11	3

After respondents were asked about their sources of information for security knowledge in their workplace, they were asked to rank their top three most useful sources of their security knowledge at workplace.

The top three sources of information security knowledge at workplace are:

- 1) Websites and search engines
- 2) Information discussions with colleagues and professional contacts
- 3) Organisation's policy.

Websites and search engines were the most popular, and it was being chosen as the most useful source of information security amongst others. The reason could be that the websites and search engines were easy to use. Moreover, the essential things to be needed in order to get the security knowledge from the source were computers and Internet access. A further factor could be due to the facilities given by most organisations being computers and Internet connections. Since respondents prefer to learn security from websites and search engines, this demonstrates how they judge the reliability of information from this channel. The information obtained could be from different sources, and anybody could put information on their blogs and websites over the Internet. This shows that respondents might not really concern the reliability of the security knowledge that they want to learn from the sources. In other words, if they had really been concerned with the reliability of information, they might have chosen academic journals or books as the main source of security knowledge.

The second most preferred source of knowledge at workplace was discussions. The discussions in this context were informal discussions among employees and their friends, including professional contacts. This informal discussion could be telephone calls, chatting online or discussions that took place during meal breaks. Some people might prefer to learn from their colleagues rather than to sit in a formal training class to gain knowledge. Hence, they might like to discuss with their friends if they have any issues that relate to security. Then, from these discussions they might grab some knowledge about information security.

In addition to that, this type of discussion is far more relaxed and does not necessarily take as long to happen. Since the possibilities that these informal discussions could happen is very high, this could be the reason why respondents found that it is a useful sources of their information security knowledge.

The third useful source as preferred by the respondents was an organisation's policy. Organisation's policy is an essential document as guidelines to control employees. As organisations are aware of the importance of information security, there are possibilities that organisations will add information about information security in their policies. This could be the rational why respondents found that this is among the top three useful sources of information security at workplace.

Respondents were asked about their preferences for future information security training. Figure 15 shows that 30% of the respondents preferred to have future security training based on the need for training, rather than a fixed schedule to undergo training. The reason might be due to the respondents' perceptions towards the importance of information security training in their daily life. The result might also be influenced by their organisations' decisions on what bases the training were conducted. However, the result represents the respondents' perceived need for themselves, rather than for their organisation. If they value the training, they will choose to have it at least on a yearly basis, and have it on demand whenever it is needed.

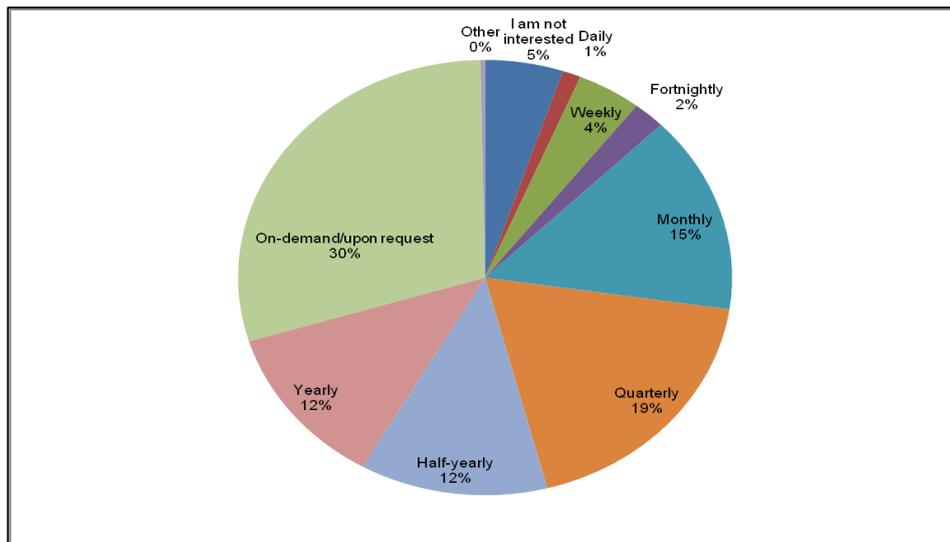


Figure 15 Respondents by their preferences for having information security training

In the survey, respondents were asked about their security practises in the workplace. There were 13 good security and 4 bad security practises listed in order to investigate what their security practises were in their office. Figure 16 shows the majority of the respondents kept their password a secret. This illustrates that they were aware that passwords should be kept as a secret as possible, and not to be shared with other people.

The second highest percentage of the security practises in the workplace was using an organisation's firewall for computer protection.

This could be due to the settings by systems administrator. This result also shows that respondents are aware that they are using firewall in their workplace. A total of 68% of the respondents used a strong password for their applications. This demonstrates that they were aware of the importance of using a strong password. However, another possibility is that the system administrator in the organisation set the password requirement according to strong password characters. The least popular security practises in the workplace was to change the password regularly. This shows that the majority of them used a strong password, did

Chapter 3 – Survey of the Transferability of Information Security Knowledge

not share their password and only a small portion of them actually changed their password on a regular basis.

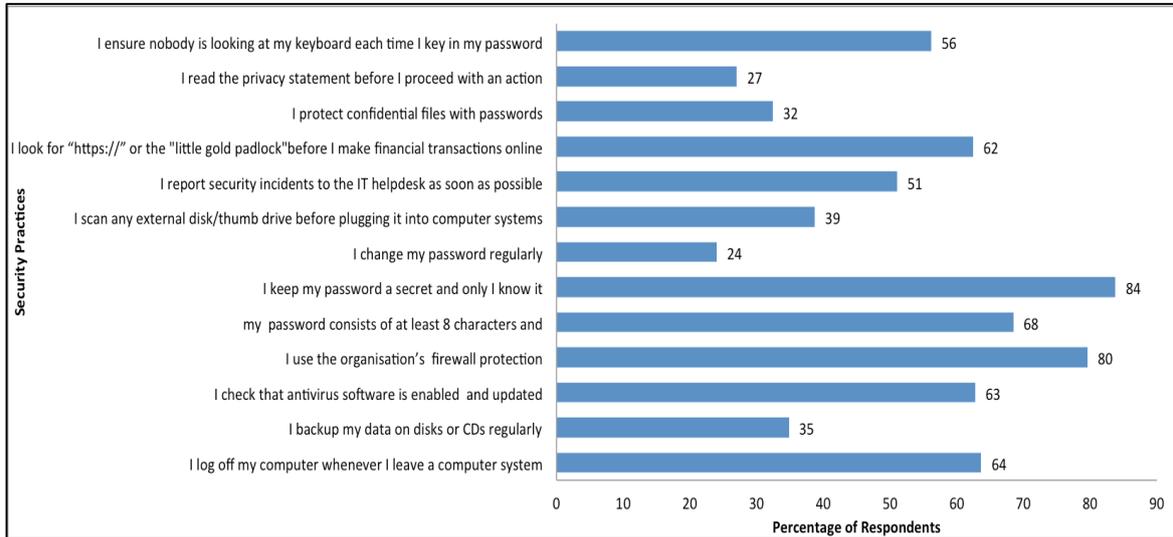


Figure 16 Percentage of respondents who answered 'Always' to the above statements (at workplace)

Apart from good security practises, respondents were asked about four negative security behaviours in their workplace.

In Figure 17, 72% of the total respondents never clicked on hyperlinks from unknown email. This, indeed, demonstrates that respondents are cautious with email coming from unknown senders. They were aware that an unknown email could contain links to websites that could auto install viruses, adware and spyware. A total of 53% of them never opened and executed files that had been attached to their email.

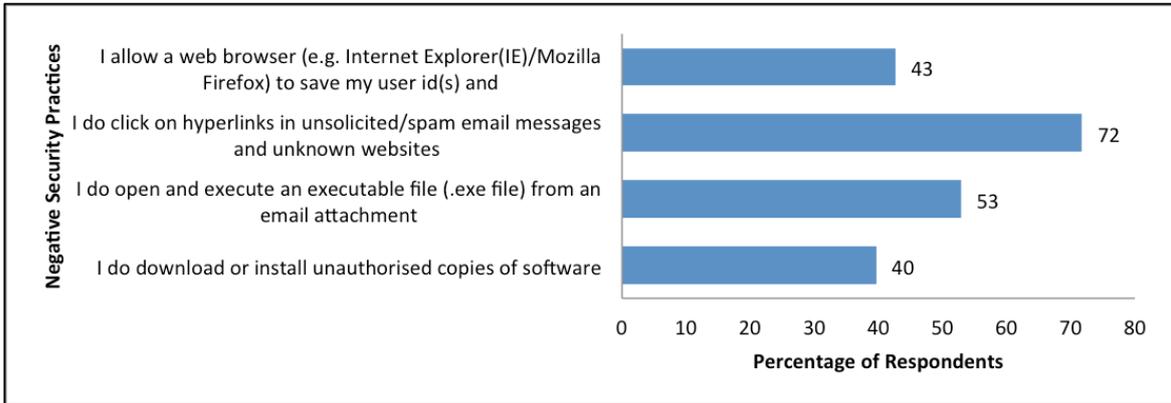


Figure 17 Percentage of respondents who answered 'Never' to the above statements (at workplace)

3.6.4 Information security practices at home

In order to compare sources of information security knowledge in the workplace and at home, respondents were asked to answer a number of questions that were similar to the previous section, but with reference to their home environment rather than the workplace. Table 8 illustrates respondents' sources of information security knowledge at home. A total of 80% of the respondents said that their sources of information security knowledge at home were from websites and search engines. This percentage also shows that about the same portion of respondents had an Internet connection at home where they could surf and obtain knowledge from the source. 37% of them said that they learned from their workplace.

Even though this percentage is not significant, it does illustrate that respondents learnt about information security knowledge at their workplace. 36% of total respondents remarked that they learnt the knowledge from daily newspaper and magazines. Since some respondents learnt from these two sources, this pointed to them being one of the mediums for disseminating knowledge of information security to family, friends and other people that stay in the same house.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Table 8 Respondents by sources of information security knowledge at home

Sources of Information Security Knowledge	No. of respondents	Percentage
Academic journals	57	17
Books	94	28
Daily Newspaper	121	36
Websites and search engines	267	80
Government or professional reports	23	7
Hearsay	67	20
Information discussions with colleagues, professional contacts	109	33
Interview	10	3
Magazines	120	36
Organisation's policy	19	6
Pamphlets/brochures	33	10
Posters	14	4
Presentation	21	6
Professional activities (conferences, meetings, briefings, etc)	35	11
Radio	46	14
Research articles	42	13
Television news	84	25
From what I learnt at my workplace	124	37

Respondents were also asked to rank their top three useful sources of security knowledge.

The top three sources of information security knowledge at home were:

- 1) Websites and search engines
- 2) From what I learnt at my workplace
- 3) Daily newspaper

Websites and search engines were chosen by respondents as the most preferred sources of information security knowledge at home. This might be because most of the respondents

have the Internet connection at home and they simply open their browser and start searching and reading about information security knowledge. Moreover, information on the websites may be updated from time to time and this might give another reason why respondents choose websites and search engines as their first rank amongst the top three sources.

The second source of knowledge preferred by respondents was their workplace. This demonstrates that respondents found that the knowledge that they had acquired in their office was useful when they were at home. In addition to this, the workplace environment might be a secured atmosphere and by being in the environment itself; respondents could gain information security knowledge from this place.

The third useful source of information security knowledge at home was daily newspapers. This could be due to the culture of people that always read newspaper every day at home. However, this source is a somewhat dubious source. At best it may alert them to particular issues that are topical at the time. It is rather unlikely to be a credible source of day-to-day advice.

Apart from the sources of security knowledge at home, the respondents were asked whether they read about security while they were at home. The result is shown in Figure 18. The majority of total respondents read about information security at home 39% monthly, 25% weekly and 7% on daily basis. Being interested in read about information security at home, indeed, was seen as a good sign of security awareness among respondents. For those who read about it on daily basis, this could be either because they needed to read it because of it being related to their job functions or they were concerned with, and interested in knowledge. On the contrary, 29% of them claimed that they did not read about it at all at home. It is suggested there may be three reasons for this; one was that they might not read

Chapter 3 – Survey of the Transferability of Information Security Knowledge

about it because they thought that it was not important for them to know about the knowledge, and second, that they might have read about it but they were not aware that the information concerned information security. The concern was how these respondents classified information security knowledge. Another possibility was that they did not know what information security was.

Respondents were asked their opinion about giving personal data over the Internet. As depicted in Figure 19, 44% of the total respondents were confident that their personal data would be protected as long as the website had specified it in its terms and conditions. This illustrates that respondents were aware that there are legal terms that could protect the privacy of their data. This also meant that they might read the terms and condition of the website if they were concerned with data privacy over the Internet. On the other hand, 34% of the respondents thought that it might be insecure to divulge their personal data on the website, even with the terms and conditions. This could be due to the possibility that the respondents were unaware of data protection on the Internet, or they simply preferred not to put their data on the websites.

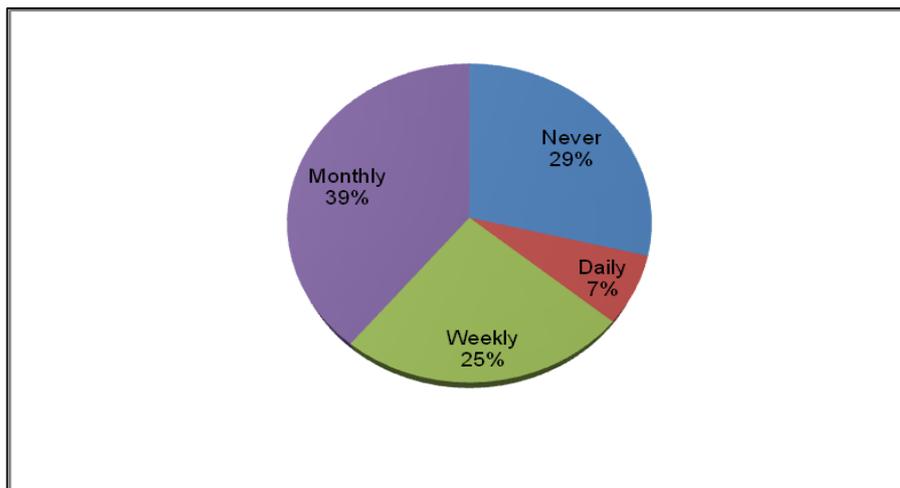


Figure 18 Respondents by how frequent they read about information security at home

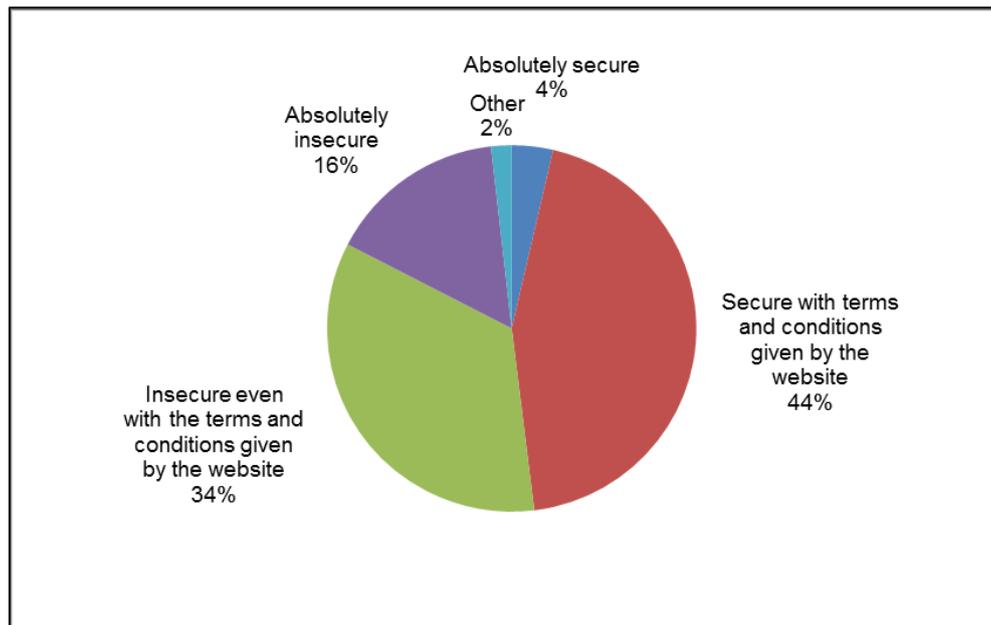


Figure 19 Respondents by their opinion on giving personal data on the websites

Social networking has become popular among the public. This application has given people another option for their social activities without having to physically exist in certain places. Amongst the respondents, 63% of them are using the application. This demonstrates that quite a number of them are using this channel to communicate and get in touch with their friends, regardless of their location. Respondents who are using social networking websites were asked about what kind of personal information that they had made available on the websites. In referring to Table 9, most of them had made their own photographs, email and their real name visible in the social networking websites. A total of 8% of them had made their full address available on the website. This shows that there are people who are not aware that putting their full address on the Internet is very dangerous. Some respondents who claimed that it was absolutely insecure to put their personal information in the website still did so.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

This information has been presented in the Table 10. From the table, it appears that even though they are aware that it is insecure to make their personal information visible, they still provide their information on the website.

This shows that if they are aware about the vulnerabilities, it does not mean that their behaviour will be in line with security practises. Logically, if they are aware that it is absolutely insecure, they should not make their full address visible.

Table 9 Respondents by their personal information that made visible in social networking websites

Personal Information	No of Respondents	Percentage (total 211)
Real Name	124	59
Email	131	62
Real date of birth	95	45
Full address	17	8
Phone number	30	14
Personal blog	47	22
Special occasions	46	22
Photographs of yourself	142	67
Photographs of your family members	78	37
Photographs of your friends	88	42
Photographs of your office	14	7
Photographs of your house	16	8
None of the above	11	5
Other	3	1

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Table 10 Respondents who said 'absolutely insecure' to put details of personal information on their social networking websites

Personal Information made available in social networking websites	No. of respondents
Real name	13
Email	16
Real date of birth	16
Full address	2
Phone number	3
Personal blog	8
Special blog	7
Photo of yourself	15
Photo of your family members	7
Photo of your friends	7
Photo of your office	1
Photo of your house	1
None of the above	2

The home environment is different from the workplace, in the sense that the owner of the house must typically protect his/her computer by him/herself. From the result of the survey, the antivirus scored the highest percentage amongst security controls. This is depicted in Figure 20. Since antivirus guards have been introduced quite a long time, and this might be the reason why most of the respondents are using it. Furthermore, most newly purchased computers come with a pre-loaded antivirus package. The second popular security controls used by respondents at home was the firewall, followed by anti-spyware. This might be because firewall and anti-spyware were introduced somewhat later than antivirus. Only 18% of respondents are using Intrusion Detection Systems (IDS) at home.

This is expected since the IDS application is merely advanced as compared to other security controls.

Moreover IDS might add other costs to the house owner, and this explains why it has scored the lowest percentage in this case. Another factor could be that the respondents are not aware that they are using IDS that includes their integrated security suite, such as Norton 360.

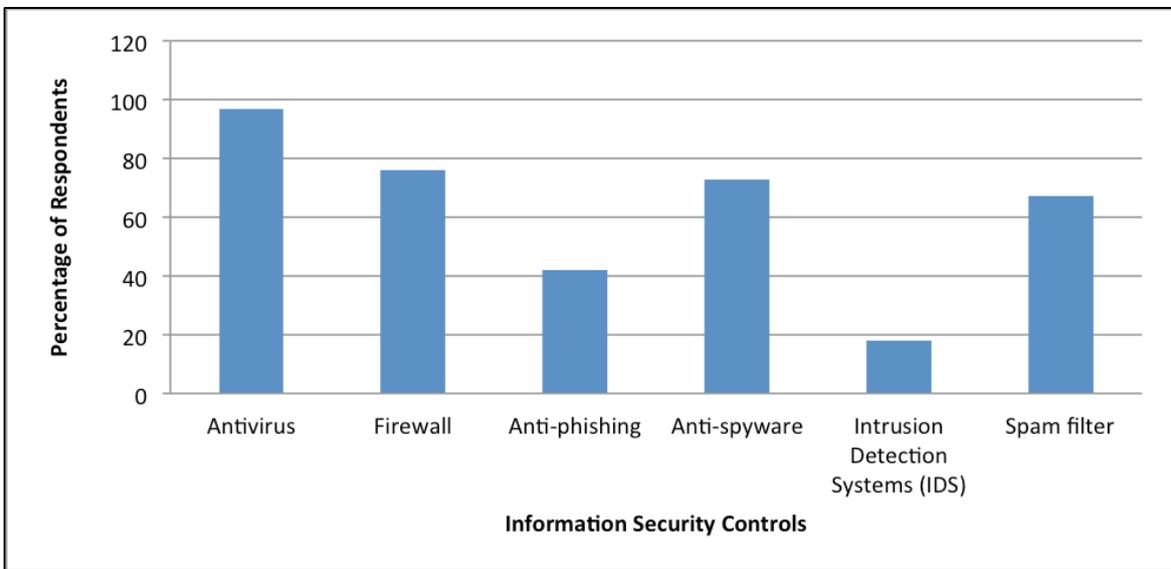


Figure 20 Percentage of respondents who are using security controls at home

In order to investigate security behaviours at home, respondents were asked similar statements as in the previous section. This is presented in Figure 21. The majority of respondents ensured that their antivirus software was enabled and updated. This illustrates that they were aware of the importance of using antivirus to protect their PC. Moving on to a second highest percentage, a total of 73% of them did not share their password with family members or friends at home. In terms of creating password, a total of 59% of them always used strong passwords when at home. Quite a good portion (63%) of them always checked on the secure connection before they made financial transactions online.

This demonstrated that they were aware and cautious whenever they were going to perform the transaction. The least popular security behaviour amongst the respondents was changing the password regularly.

This could be due to there being no policy for changing passwords being implemented at home. Shredding confidential information before throwing it was a common practise at workplace. Astonishingly, about 45% of total respondents shredded their confidential information at home. This shows that they were practising what they had learnt at workplace even when they were at home.

Apart from the above good security behaviours, the respondents were asked about four poor security behaviours at home. This information is demonstrated in Figure 22. A total of 68% of them never clicked on links being sent in spam email and unknown websites. In terms of opening and executing files from email attachment, 54% of them claimed that they never do it. About 31% and 38% of them never download unauthorised software and allow a web browser to remember their password respectively. The results reveal that those users are actually practising certain information security behaviours when they are at home.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

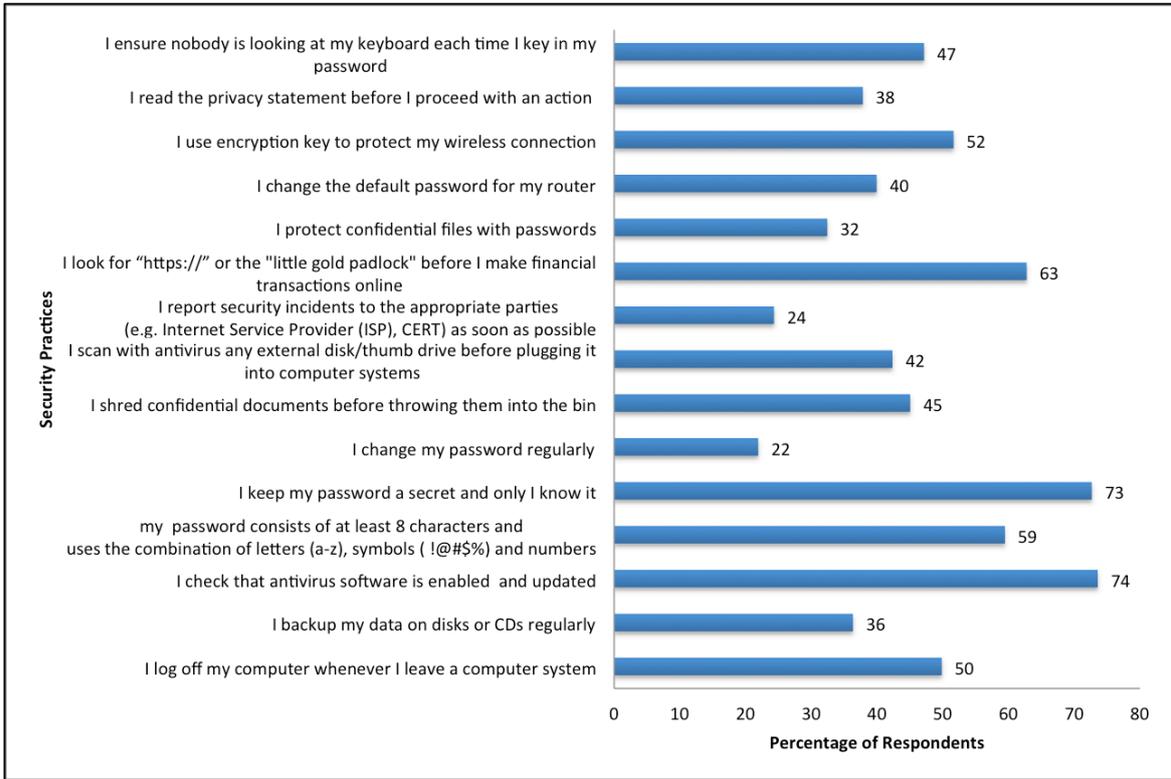


Figure 21 Percentage of respondents who answered 'Always' to the above statements (at home)

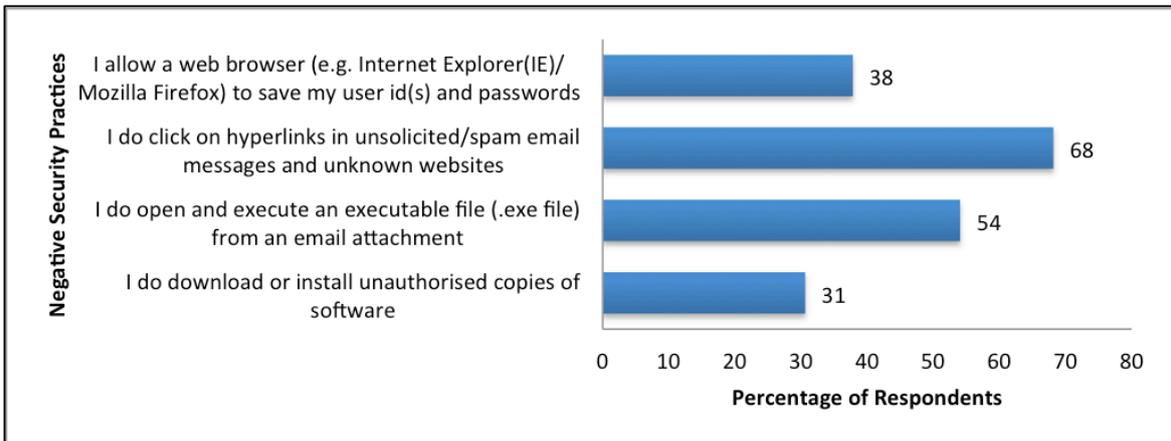


Figure 22 Percentage of respondents who answered 'Never' to the above statements (at home)

3.6.5 Effectiveness of information security training

Information security training is a method of raising users' information security awareness level. In this survey, 118 (35%) of the 333 respondents attended training in their workplace.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

This group of respondents was analysed separately in order to see the impact of training towards the respondents. Those who received information security training with their security awareness level are illustrated in Figure 23. The majority of them (39%) claimed as having high, followed by 27% as very high and 29% as an average level of awareness. This is to be expected since they had undergone such training, and 66% of them had an above average level of awareness.

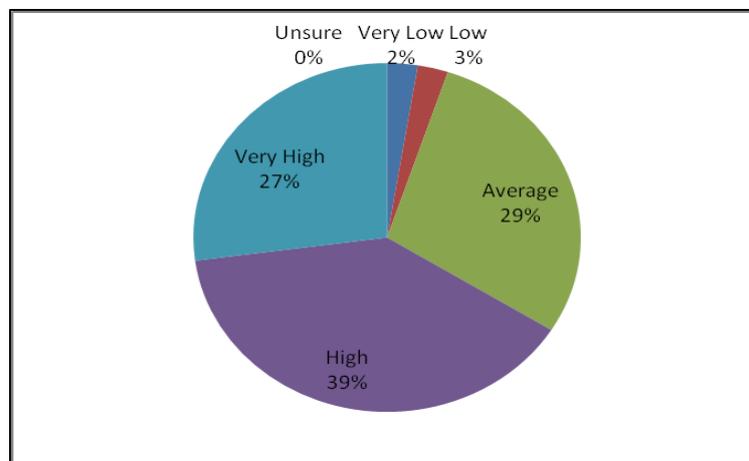


Figure 23 Respondents who attended training and their awareness level

What respondents thought about them as having a high and very high awareness level does not mean that they were aware about security. Therefore, who they thought was responsible for information security tasks could show whether they really understood individual security responsibilities after undergoing security training. Figure 24 illustrates the percentage of respondents and their understanding of security responsibilities. The majority of them considered that the system administrator should do all the information security work. A total of 59% of them commented that it was the individual's responsibility to take care of security role. Only 2% of them did not know who should take on the security responsibility.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

This, indeed, shows that more than half of those who attended training understood that every individual should take part in securing their information.

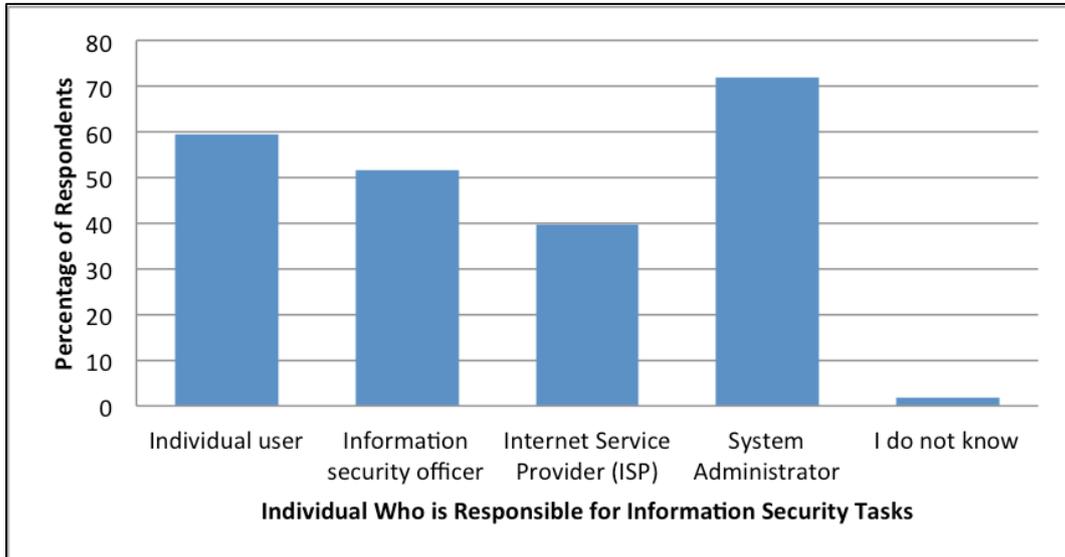


Figure 24 Percentage for who respondents (received training) think is responsible for information security tasks

The result has been analysed based on training type in order to see which training type favoured most by organisations. The majority of respondents who attended training are from organisations that have more than 1000 employees, as shown in Table 11. Overall, this type or organisation scored the highest percentage for each type of training, as compared to the others.

From the same table (see Table 11), it may be seen that organisations with more than 1000 employees prefer to conduct in-house training with insider experts. This could be because they have budgets to invest trainings for experts and conducted their own training in the future. Apart from taking into account the percentage of organisations that have more than 1000 employees, organisations with less than 50 employees conducted their in-house training by inviting outside experts. This could be due to budget constraints and less experts

Chapter 3 – Survey of the Transferability of Information Security Knowledge

in the organisation. The table also exhibits that small medium enterprise (SME) provide security trainings for their employees.

Table 11 Respondents by training type and size of organisation

Size of organisation	Training type					
	In-house by insider experts	In-house by outside experts	Outside the organisation	Self-study	Online training	Other
1-49 employees (%)	10	24	15	14	14	0
50-99 employees (%)	0	3	8	6	5	0
100-250 employees (%)	18	13	18	11	11	0
251-499 employees (%)	6	11	8	6	8	67
500-999 employees (%)	4	8	8	7	3	0
1000+ employees (%)	62	42	45	56	59	33
TOTAL	100	100	100	100	100	100

In order to see the impact of security training, those who attended training could be assumed as having a good understanding of security terms as compared to those who did not. Referring to Table 12, respondents who had undergone security training did score a higher percentage than those who did not, except for the two fake security terms. In this case, the percentage of those with training was expected to be less because these terms did not exist

Chapter 3 – Survey of the Transferability of Information Security Knowledge

in the information security area. However, this differed where respondents who did not undergo training were better and more honest in answering the questionnaire.

A further reason could be the respondents who had training might think that they had come across these terms, and were trying to claim that they understood all the security terms.

Table 12 Respondents who understand the below security terms

Information Security Terms	Respondents who received training (%)	Respondents who did not received training (%)
Virus/Worm	97	90
Trojan horse	93	73
Spam	94	87
Social engineering	58	35
Phishing	81	64
Pharming	34	19
Identity theft	85	79
Key loggers	72	48
*Phlopping	10	5
Botnets	50	24
Zombies	50	24
Denial of service	75	47
Packet sniffer	65	37
*Whooping	16	7
Hacker	97	94
Zero day attacks	45	21
Cracker	74	46

*Fake security terms

Chapter 3 – Survey of the Transferability of Information Security Knowledge

The results for information security practises have been analysed based on those who received or attended trainings in their workplace and those who did not. These results have been separated into three different tables:

- a) Table 13 Respondents by their good information security practices (based in who answered 'Always' at workplace and home)
- b) Table 14 Respondents by their negative security practices (based on who answered 'Never' at workplace and home)
- c) Table 15 Respondents by their good information security practices at home (based on who answered 'Always')

Referring to Table 13, the overall result shows that percentage of those who attended training is higher than those who did not. This demonstrates that training in the workplace does have a good effect on those who could attend the training.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Table 13 Respondents by their good information security practices (based in who answered 'Always' at workplace and home)

Good Security Practices	Respondents who received training (%)	Respondents who did not receive training (%)
I log off my computer whenever I leave a computer system	50	36
I backup my data on disks or CDs regularly	34	26
I check that antivirus software is enabled and updated	68	53
I use the organisation's firewall protection	72	60
My passwords consists of at least 8 characters and uses the combination of letters (a-z), symbols (!@#)\$%) and numbers (0-9)	71	47
I keep my password a secret and only I know it	85	62
I change my password regularly	24	9
I scan with antivirus any external disk/thumb drive/USB drive when first plugging it into the computer system	42	26
I report to security incidents to the appropriate parties	33	16
I look for "https://" or the "little gold padlock" before I make financial transaction online	60	54
I protect confidential files with passwords	36	20
I read the privacy statement before I proceed with an action (such as registering with a website, installing an application or financial/online banking transaction)	34	18
I ensure nobody is looking at my keyboard each time I key in my password	56	35

The most common practise of respondents at home and workplace was to keep their password secret. This was because it is a simple practise and easy to understand the reason why they should not tell other people about their password. It is like telling others that they should keep their secret to themselves. Another possible reason might be because the password is essential to most computers and Internet applications. Therefore, most respondents might be using passwords in their daily operations.

On the other hand, the least common practise at both environments is changing their passwords regularly. This shows that even though they used passwords to protect their systems or applications, only a small portion of the respondents actually changed their passwords regularly. Even for those who had received training, there were 24% of them who did not change their passwords regularly. These respondents might have been aware that they should change their password from to time but they just ignored it. A further factor might be that the system administrator did not set the rules that enforce users to change their password regularly.

Based on the same table (see Table 13), there is one statement that asked about “https://”. This statement was designed to ascertain whether respondents were being aware of the secure connection of the website before they proceeded with financial transactions. 54% of those who did not receive training checked the validity of the website before proceeding to the secured transaction. This showed that respondents were concerned with their financial transactions and resulted in this good practice. In addition to that, this might be sign that the awareness message about how to protect themselves from being a victim of phishing and pharming attacks has reached the respondents without having to undergo formal training.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Among the security practises statements, there are four negative security behaviours. In this case, the correct answer should be 'Never' instead of 'Always' like the above table. These results have been illustrated in Table 14. In this table, the respondents who attended security training should have lower percentage compared to those who did not. However, there were two negative security practises that had a higher percentage for those who have received training; 'I do open and execute an executable file (.exe) from an email attachment' and 'I allow a web browser (e.g. Internet Explorer (IE)/Mozilla Firefox) to save my user id(s) and passwords for faster access in the future'. For the first, 'I do open and execute the executable file....' there it is possible that they actually opened the executable files, because they might think that since the computer systems at workplace is protected, then it was acceptable to open the file. They might think that if anything were to happen, the system administrator would take care of it. Another possibility is that the awareness message in the workplace did not indicate that the users are not supposed to open any unknown attachment or executable files from their email. For the second practises 'I allow a web browser to save my user id(s)....' it might be because respondents are busy in their workplace and prefer to save their usernames and passwords using their web browser. If in their workplace people are sharing a computer with the same username, then it is actually dangerous to practise such behaviour. Overall, the gap in the percentage between those who received training and those who did not was, indeed, very small. Since most of the statements in the question were good security practise, this could lead to confusion for the respondents if they did not pay attention while answering the questions. It is either they are really answering the question based on their practises or they might confused due to the positive security practises statements beforehand, or they are not paying their attention while answering the question.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Table 14 Respondents by their negative security practices (based on who answered 'Never' at workplace and home)

Negative Security Practices	Respondents who received training (%)	Respondents who did not receive training (%)
I do download or install unauthorised copies of software	25	27
I do open and execute an executable file (.exe file) from an email attachment	47	46
I do click on hyperlinks in unsolicited/spam email messages and unknown websites	60	62
I allow a web browser (e.g. Internet Explorer (IE)/Mozilla Firefox) to save my user id(s) and passwords for faster access in the future	41	30

Table 15 below, demonstrates three good security practises were asked regarding home security practises. The table shows comparisons of good security practises in the home by respondents who answered 'Always' for these three practises. These percentages were calculated based on respondents who received training and who did not attend training in their workplace. For these three practises, the percentage of respondents who received training was higher than those who did not receive information security training. This illustrates that information security training in the workplace does improve respondents' security behaviour at home. They were aware and practised security behaviour even though there was no policy at home to enforce them to observe these three practises. This also shows that there is a transferability of security knowledge from their workplace to the home environment.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Table 15 Respondents by their good information security practices at home (based on who answered 'Always')

Good Security Practices	Respondents who received training (%)	Respondents who did not receive training (%)
I shred confidential documents before throwing them into the bin	50	42
I change the default password for my router	53	33
I use encryption key to protect my wireless connection	59	47

Since security training should give greater awareness in terms of privacy issues, respondents who attended training should have been more aware of the privacy terms and condition on the website. Surprisingly, 46% of those who did not attend training scored better in percentage terms, as compared to those who attended, as shown in Table 16. This shows that the topic of security training in terms of privacy issues could be improved in this case.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Table 16 Comparison of respondents by their opinion about giving personal data on websites

Opinions	Respondents who received training (%)	Respondents who did not receive training (%)
Absolutely secure	5	3
Secure with terms and conditions given by the website	42	46
Insecure even with the terms and conditions given by the website	34	35
Absolutely insecure	19	13
Other	0	3

In terms of backing up data on PC, the percentage of those who had undergone training was higher by 12%, as compared to those who did not, as shown in Table 17. Astonishingly, a total of 63% of those who did not receive training did their backup at home. This illustrates the fact that respondents were aware of the importance of making a backup for their data on personal computer.

Table 17 Comparison of respondents who backup their data on personal computer at home

	Respondents who received training (%)	Respondents who did not receive training (%)
Yes	75	63
No	25	37

Since the respondents had undergone training, they should have been using information security control more, as compared to those who had not.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Referring to Table 18 below, most of the respondents who received training scored higher as compared to those who did not. However, these results suggest that training does give a good impact to those who attend it. It is good to observe that although the respondents did not attend training, they were aware of the importance of using security controls at home. Furthermore, the gap in percentages between these two groups was not really high. This suggested that in terms of using security controls, more than half of the total respondents used antivirus, firewalls, and anti-spyware regardless, whether they had undergone security training or not.

Table 18 Comparison of respondents who answered 'Yes' to the below security controls at home

Security Controls	Respondents who received training (%)	Respondents who did not receive training (%)
Antivirus	98	97
Firewall	79	74
Anti-phishing	44	40
Anti-spyware	74	72
Intrusion Detection Systems (IDS)	19	17

3.7 Conclusion

Based on the previous discussions, it may be seen that in terms of information security awareness, 49% of total respondents claimed that they had an above average level of security awareness. However this portion does not really represent their actual security awareness, since those who have claimed to have an average level are better at recognising fake security terms.

The results for recognising security terms have shown that respondents are aware of the terms hackers, virus/worm and spam. In addition to this, respondents were quite aware of the importance of using security control protection at home by using most of the security controls specified in the questionnaire. 36% of respondents' organisations provided training to its employees. This could be seen as one of the efforts to raise security awareness among employees.

In relation to this, results show that the majority of respondents attended security trainings on a yearly, monthly and quarterly basis.

In terms of the method of training that they had undergone, the majority of them experienced self-study and in-house training by insider experts. In addition to this, security topics that had been asked in the questionnaires were taught in this training. Below are the security topics taught in the training arranged by the most popular and the last topic as the least:

- 1) Security policy of the organisation & Network Security
- 2) Access control systems
- 3) Security and risk management
- 4) Impact of security breaches on the organisation
- 5) Physical and environmental security issues
- 6) Legal issues
- 7) Secure communication

From the above topics, it may be seen that organisations are deeply concerned about security policy and network security that resulted in the first popular topic in the trainings provided. However, all of the above topics are, indeed, important in order to educate and raise awareness levels amongst employees.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

The majority of the respondents received training via presentations. This illustrates that presentations have become the main method of delivering security training for the respondents. In addition to this, the second and the third method (two methods with the same score) experienced by most of the respondents were email alerts and handbooks and web-based awareness courses. Hence these methods could be a possible approach to building security awareness programmes in the future.

Furthermore, the respondents learnt about security through various sources when they were at the workplace and at home. As shown in Table 19, the sources are arranged based on the highest percentage of respondents to the lowest.

Referring to Table 19, the main sources of security knowledge at both contexts are websites and search engines. Based on the results in the table, the second main source of security knowledge at home is what they have gained at workplace. This, indeed, shows that the workplace is one of the places where people could learn about security knowledge. Apart from websites and search engines, most of the sources of knowledge at home are quite informal such as daily newspapers, magazines and television news. On the other hand, main sources in the workplace are more formal, in the sense that respondents learnt from organisations' policy books, professional activities and academic journals.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

Table 19 Comparison of sources of information security knowledge between workplace and home

Number	Sources of information security knowledge	
	Workplace	Home
1	Websites and search engines	Websites and Search engines
2	Information discussion with colleagues, professional contacts	From what I learnt at my workplace
3	Organisation's policy	Daily Newspaper and Magazines
4	Books and Magazines	Information discussions with colleagues, professional contacts
5	Professional activities	Books
6	From what I learnt at home	Television news
7	Academic journal	Hearsay
8	Presentation and Daily newspaper	Academic journals
9	Research articles	Radio
10	Hearsay	Research articles
11	Pamphlets and brochures	Professional activities
12	Government or professional reports	Pamphlets/brochures
13	Posters	Government or professional reports
14	Television news	Presentation and Organisation's policy
15	Radio	Posters
16	Interview	Interview

Chapter 3 – Survey of the Transferability of Information Security Knowledge

The respondents prefer to learn from websites and search engines in both environments, as shown in Table 20. In their workplace, respondents found that information discussions with colleagues and their professional contacts are very useful next to the websites and search engines. In addition to this, they also preferred to learn security knowledge from the organisation’s policy. On the contrary, respondents found that what they had learnt in the workplace was actually beneficial to them. Moreover, daily newspaper seemed to be among the top three preferable sources at home. In terms of preferences of having security training, the majority of them preferred to have this on demand.

Table 20 Comparison of the top three sources of information security knowledge at workplace and home

Rank	Source of information security knowledge	
	Workplace	Home
1	Websites and search engines	Websites and search engines
2	Information discussions with colleagues and professional contacts	From what I learnt at my workplace
3	Organisation’s policy	Daily newspaper

The results of the survey suggest that there is a transferability of information security knowledge for both the workplace and home. The difference between these two contexts is that the amount of knowledge being transferred from the workplace is greater, compared to the other direction. This has been shown in Table 20, where the majority of respondents chose: ‘From what I have learnt from workplace’ as the second main source of knowledge at home. In contrast, whilst in the workplace, the respondents selected ‘From what I learnt at home’ as the sixth main sources of their security knowledge at workplace.

Chapter 3 – Survey of the Transferability of Information Security Knowledge

In addition to this, the result shows that respondents practising information security behaviours at home could be considered as transferability of knowledge between the workplace and the home.

The survey results also demonstrated that people have their preferences when asked about their top three sources of information security knowledge. For example, respondents like to learn from websites and search engines, informal discussions with colleagues, organisation's policy and newspapers. These preferences would potentially help to motivate them to learn about information security. Therefore, education and learning preferences are discussed in the next chapter.

4 Education and Learning Practices

4.1 Introduction

Learning has been defined as the “human process of creating meaning from experience” (Watkins, 2010). Dictionary defines learning as ‘the activity of obtaining knowledge’ (Cambridge University Press, 2011). Learning comprises of two meanings: (1) the acquisition of skill or know-how, which implies the physical ability to produce some action, and (2) the acquisition of know-why which implies the ability to articulate a conceptual understanding of an experience (Kim, 1998). Kim (1998) further defined learning as increasing one’s capability to take effective action; operational; and conceptual. Abbot (1994) defined learning as

“reflective activity which enables the learner to draw upon previous experience to understand more comprehensive definition of learning as:

1. An active process involving accommodation and assimilation of ideas, skills, thoughts and so on.
2. Involve past, present and future interconnections
3. A process that is influenced by the use of learning itself.”

Lahey’s (2004) definition, meanwhile, is:

“..to qualify as learning, change in behaviour must be brought about by interaction of a person with his or her environment. Thus, learning can be defined as any relatively permanent change in behavior, knowledge, and thinking skills, which comes about through experiences.”

Therefore, learning can be defined as a process of acquiring knowledge which involves understanding the past, present and future interrelated experiences, resulting in a change of behaviour and skills. In the learning process, pedagogy is one of the methods to teach people, and this has been implemented in schools (Coffield *et al.*, 2004b). Pedagogy is defined as ‘the art and science of teaching children’ (Knowles, 1988). The term ‘Pedagogy’ is taken from Greek word “paid” (boy) and “agogus” (guide) which refers to “the method and practice of teaching”(Oxford Dictionaries, 2012).

4.2 Information security awareness and practices through education

Little research has been done on information security awareness and pedagogy approach.

Karjalainen and Siponen (2011) have reviewed existing information security trainings and proposed four pedagogical approaches in designing and evaluating information systems security training. The four pedagogies are:

1. The explicit psychological context must be based upon the group-oriented theoretical approach of teaching and learning – the explicit psychological context here means humanistic psychology, which includes behaviourism, cognitivism and constructivist emphasises on individual learning. The authors proposed it to be group oriented approach, because they believe that employees’ compliance with Information Systems (IS) security procedures is not enough at the individual level to ensure the organisational success.
2. The training content must be based on the collective experiences of the learners – the authors highlighted that the information security training contents should include learners’ collective experiences and perceptions. With this, the authors believe that employees would agree, understand, accept and implement IS security policies that are more community centred.

Chapter 4 – Improving the Information Security Awareness and Practices through Education

3. Teaching methods must focus on collaborative learning in order to reveal and produce collective knowledge – the authors stress the need of collaborative learning in teaching, because they believe that it will enable communal change in employees' attitudes and behaviour. The learners should provide opportunities to discuss their experiences, attitudes and behaviour towards information security issues.
4. Evaluation of learning should emphasize experiential and communication-based methods from the viewpoint of the learning community. - the authors suggest the possible evaluations for the IS security training are formal exams (such as multiple choice styles answers tests), competence based evaluations, peer evaluations, assignments, interviews and group projects.

These four pedagogies are biased towards organisation's implementation, and the authors specifically mention that their target audience will change employees' IS security attitudes and behaviours. For example, the employees are expected to comply with the IS security procedure in this case. However, this pedagogical approach could be adopted to teach the general public. For instance, rather than expecting people to comply with IS security procedures, they may be expected to practice the guidelines to secure home computers. Even though the research is meant to be for information security training, not for awareness education, it has been reviewed in this research because the study's aim is to change employee's behaviour which is the similar aim as security awareness is (NIST, 2003).

Yuen-Yan and Wei, (2009) used conceptual change pedagogy for information security awareness education. Conceptual change is defined as "a process that revises a student's understanding of a topic in response to new information" (Yuen-Yan and Wei, 2009). In the study, the author has two groups (experimental and control) of non-engineering undergraduates students from the Chinese University of Hong Kong.

Chapter 4 – Improving the Information Security Awareness and Practices through Education

Both groups were asked to rank eight statements (pre-test) about information security beliefs. An example of one of the statements is “When we use Internet banking services, we should make sure the connection is SSL-enabled”. The participants then attended a lecture covering the topics of Web security, computer safety and network security. The experimental group was presented a demonstration on how the Secure Socket Layers (SSL)-enabled webmail contents could be sniffed and encrypted. The group were asked Q1: “When we send and receive emails via (the webmail application) it’s possible for eavesdroppers to read the messages’ content. Is it true? (yes, no, I don’t know)”. Then, the second demonstration was presentation on also SSL-enabled webmail but showing part of the website contents that is not encrypted. The group was then asked the same as Q1, to ensure if the conceptual conflict created could be beneficial in teaching information security. In the end, the participants were asked to re-ranked the eight statements again (post-test) to see if they had learnt from the demonstrations. The control group were given demonstrations to illustrate the packet sniffing of several SSL-enabled sites and the non SSL-enabled and explain directly the differences between the two. The results show that the experimental participants were able to understand the security concept being presented to them better than the control group. In the research, they found that using pedagogy for non-engineering undergraduates students was effective. The research was, however, limited to non-engineering undergraduates students whereas it would be more interesting if the study could include all group of students as they would be representing the whole university population. A positive aspect of the research was the experiment methods, since the authors chose to have pre and post-tests to compare improvements in the participants.

4.3 Learning styles

Each individual has his/her own way of learning (Guldborg, 2004; Pritchard, 2005; Gilbert and Swanier, 2008). One can have more than one learning style.(Fleming, 2006)

Chapter 4 – Improving the Information Security Awareness and Practices through Education

Learning styles have been defined in different words by researchers:

“a description of the attitudes and behaviour which determine an individual's preferred way of learning”(Honey and Mumford, 1992),

“an individual's preferred approach to organising and presenting information” (Riding and Rayner, 1998)

“the way which learners perceive, process, store and recall attempts of learning” (James and Gardner, 1995).

“distinctive behaviours which serve as indicators of how a person's mind operates” (Gregorc, 1979).

“personal manners to perceive and process information, and how they interact and respond to educational stimuli” (Alonso, 1993).

Hence, from the above definitions, learning styles may be defined as an individual's preferred ways of learning, which depends on how learners perceive, process and present the information.

Research in learning styles is conducted in different areas and disciplines, such as medical and health care training, law, management, industry, vocational training, agricultural and education (Cano *et al.*, 1992; Abbot, 1994; Boyle and Dunn, 1998; Entwisle, 2001; Cassidy, 2004; Breckler *et al.*, 2009). However, little research has been done in the area of learning styles in security education (Yurcik and Doss, 2001; Crowley, 2004).

Chapter 4 – Improving the Information Security Awareness and Practices through Education

The literature review will therefore focus upon general approaches to learning styles.

Coffield et al. (2004b) classified learning styles into five big families.:

- 1) The first family is learning styles and preferences that are largely constitutionally based, including the four learning sensors; visual, auditory, kinaesthetic and tactile (VAKT). This family is more genetically influenced by personality traits / the dominance of sensory or perceptual channels / the dominance of certain functions related to the left or right brain.
- 2) The second is learning styles that reflect cognitive structure such as patterns of ability. The family link learning styles to personality features, with the implication that cognitive styles are deeply embedded in personality structure.
- 3) The third is learning styles in relation to stable personality type. The theorists in this family believe that personality traits contribute strongly to the learning styles of individual.
- 4) The fourth is learning styles which are flexibly stable. The theorists in this family follow Kolb's learning theory, whereby "learning style is not a fixed trait, but a differential preference for learning, which changes slightly from situation to situation. At the same time, there is some long-term stability in learning style" (Kolb, 2000).
- 5) The fifth group of learning styles includes learning approaches, strategies, orientations and conceptions of learning. Theorists in the family focus on the personality differences and fixed cognitive characteristics.

See Figure 25 below, the learning styles models that are in bold are the most influenced models amongst the 51 that relate to the field of post-16 learning styles. The 13 models that have been reviewed in detailed are based on validity, reliability and practical application.

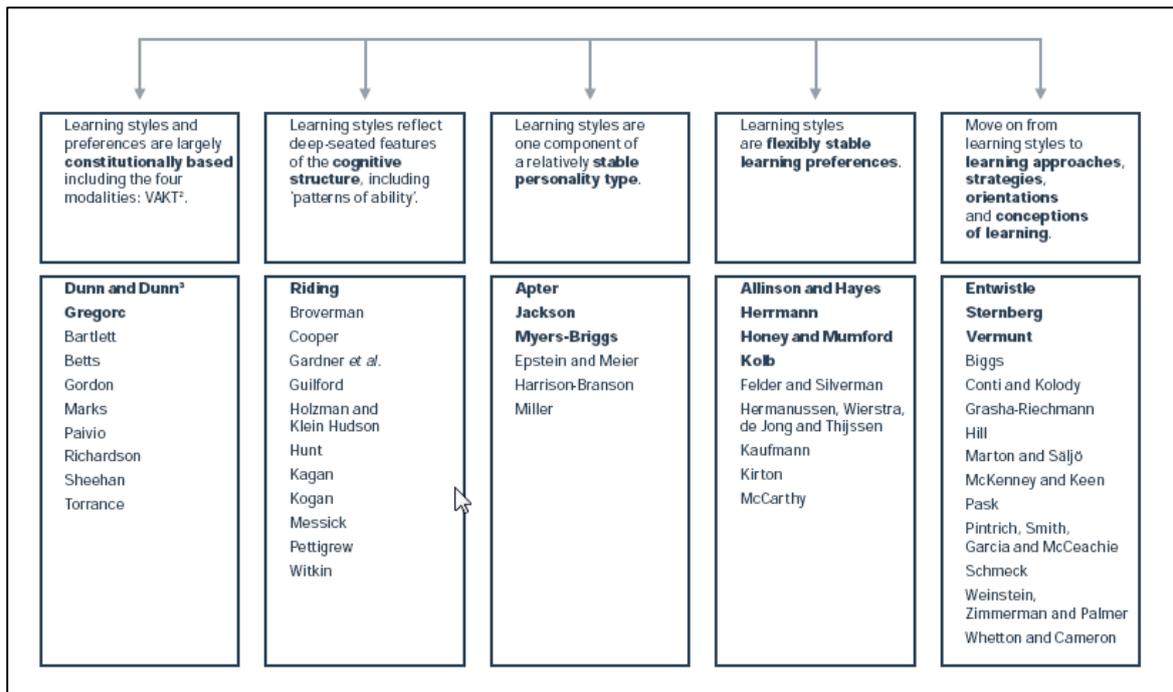


Figure 25 Families of learning styles (Coffield *et al.*, 2004a)

* Source: (Coffield *et al.*, 2004b)

4.3.1 Learning styles in adult education

Adult education has been defined as ‘the practice of teaching and educating adults’ (Blakely and Tomlin, 2008). A similar term referred to in adult education is Andragogy. Andragogy is ‘the science of understanding theory and supporting practice lifelong and life wide education of adults’ (Reischmann, 2004). Since one of the objectives of this research is to improve information security practices within organisation via educating staff and also the general public, it is worth reviewing learning styles that have been used by other researchers in adult education. In referring to Table 21 below, a number of researchers use more than one type of learning style in their research, to maximise the learning process.

Chapter 4 – Improving the Information Security Awareness and Practices through Education

Table 21 Learning styles in adult education

Researcher	Learning Styles	Comments
(Vincent and Ross, 2001b)	<ul style="list-style-type: none"> • Multiple intelligence (Gardner, 1993) • Sensory Learning Styles - Visual Auditory Kinaesthetic (VAK) (Kanar, 1995) 	Suggested that learning should be personalised by incorporating learning styles VAK and multiple intelligence. Learning styles will benefit learners and as well as trainers.
(Gilbert and Swanier, 2008)	<ul style="list-style-type: none"> • Felder and Silverman learning styles (Felder and Soloman, 2009). 	One can have many learning styles depends on course objectives or subjects. When objective of learning change, the learning styles might change too, for example, when solving equation, visual styles is preferred. The learning styles was used effectively in the Engineering and the sciences.
(Kinshuk and Taiyu Lin, 2003)	<ul style="list-style-type: none"> • Felder and Silverman Learning Styles (Felder and Silverman, 1988) 	Developed a prototype of PHP programming course based on the learning styles.
(Novak, 2006)	<ul style="list-style-type: none"> • Grasha-Reichmann Student Learning Style Scale (GRSLSS) (Grasha, 1996) 	GRSLSS was chosen because it focuses on social interaction between facilitator, students and other students. It also described the teaching style environments.
(Pigg <i>et al.</i> , 1980)	<ul style="list-style-type: none"> • Kolb's Learning Styles Inventories (Kolb, 1981) 	The learning styles inventories are useful in conducting adult educational programme.
(Mustaro and Silveira, 2006)	<ul style="list-style-type: none"> • Multiple Intelligence Inventory (Gardner, 1993) • Kolb Learning Styles Inventories (Kolb, 1981) • Felder and Silverman Learning Styles (Felder and Silverman, 1988) 	Learning styles used for adult learning in learning object. Learning object is any digital entity which can be used, reused or referenced during a technology-mediated learning process (Wiley, 2000).
(Burke and Doolan, 2008)	<ul style="list-style-type: none"> • Dunn and Dunn Learning Styles (Dunn and Dunn, 1978) 	Presented research done in 47 institutions of higher education that use Dunn and Dunn learning styles. He found that sociological and biological uniqueness that makes each individual learn differently. He also suggested that lecturers and professors in higher education institutions should aware on student's learning style as this the essential method toward improving academic achievements.

Chapter 4 – Improving the Information Security Awareness and Practices through Education

Researcher	Learning Styles	Comments
(Materna, 2007)	<ul style="list-style-type: none">• Sensory Learning Styles-VAKT (Materna, 2007)• Kolb's Learning Styles (Kolb, 1981)• Multiple Intelligence Inventory (Gardner, 1993)	Suggested the three learning styles to be applied in adult education.

All the researchers above agree that each individual has his/her own preferences in learning. Learning styles may not be the main determinant of learners' achievement, but will enhance and make the learning process easier and interesting. For example, learning styles help individual learns efficiently and effectively (Vincent and Ross, 2001b; Kratzig and Arbuthnott, 2003). Furthermore Davis (2007) agrees that learning styles could create the ultimate learning experience to the learners. There are many other learning styles models. However, this research will choose learning styles that are suitable for adult learning.

4.3.2 Human Sensory Learning Styles

According to Kanar (1995), there are three types of learning style, related to human sensor; auditory (hearing), visual (picture) and kinaesthetic (physical). Gentry (1990) refers to learning styles in the same terms as visual, auditory, kinaesthetic, with the additional term 'tactile'. Another researcher also uses the same terms, with the additional of 'reading and writing' as in VARK learning styles (Fleming and Bonwell, 2001). In summary, these three learning styles (visual, auditory and kinaesthetic) are the most common learning styles referred by researchers and applied at schools, universities and workplace (Lujan and DiCarlo, 2006)

An auditory person like listening and talking, outgoing personalities (talkative), and does not prefer reading written instructions (Kanar, 1995). Vincent and Ross (2001a) suggest the teaching materials that are suitable for an auditory person are to create auditory tapes of class notes and chapters and let them listen to them.

Chapter 4 – Improving the Information Security Awareness and Practices through Education

Encouraging them to participate in a class discussion which involves asking and answering questions sessions is also a good strategy for them. Teachers or students are also encouraged to read out loud chapters in class. When self-studying, an auditory person may whisper new information or chapters to themselves.

A visual person is usually quiet; he/she prefers picture, high imagination ability and having problems with verbal instructions. These people memorise things in pictures and images (Kanar, 1995). Presenting information in the form of videos, charts and pictures is a good way of teaching them. In schools, teachers using bright and colourful ink to prepare their teaching materials for visual learners (Vincent and Ross, 2001a).

Whilst auditory and visual person learn by listening and picturing respectively, kinaesthetic students learn by actions. Kinaesthetic learning may be defined as 'using one's body to physically touch or manipulate objects or materials' (Breckler *et al.*, 2009). They usually express themselves physically and have an outgoing personality. They are also poor listeners, as they need to touch and feel in order to understand. In a traditional classroom, these learners find very difficult to concentrate as they are a hands on person (Vincent and Ross, 2001a). It is suggested that they should write notes while listening to a lecture and underline important information while reading books or written resources. Vincent and Ross (2001a) also suggest that they should develop projects to help them conveying their ideas. Hawk and Shah (2007) suggest that kinaesthetic learners could be taught by creating a field trip, use trial and error, and create an experiment in laboratories and practical sessions.

4.3.3 VARK Learning Styles

VARK is an acronym originating from the initial letters of four sensory modalities that are used for learning information (Visual, Aural, Read/write and Kinaesthetic), and was developed in New Zealand in 1987 by Flemming (Fleming, 2006). People use these four modes to receive and give information. For example, some people like to 'read' texts rather than looking at 'diagrams'. Others like to 'listen' to a lecture rather than 'doing' practical session. These preferences may be represented by VARK modes in identifying people's learning styles. These four modalities have been defined by Flemming (2006):

“Visual (V): This preferences includes the depiction of information in charts, graphs, flow charts, and all symbolic arrows, circles, hierarchies and other devices that teachers use to represent what might have been presented in words. Layout, whitespace, headings, patterns, designs, and colour are important in establishing meaning. These students are more aware of their immediate environment and their place in space. It does not include pictures, movies, videos and animated websites (simulation) that belong with Kinaesthetic below.

Aural (A): This perceptual mode describes a preference for information that is spoken or heard. Students with this modality report that they learn best from discussion, oral feedback, email, cellphone chat, discussion boards, oral presentations, classes, tutorials and talking with other students and teachers.

Read/write (R): This preferences is for information displayed as words either read or written. Not surprisingly, many academics and high-achieving students have a strong preference for this modality. These learners place importance on precision in language, and are keen to use quotes, lists, texts, books and manuals. They have a strong reverence for words.

Kinesthetic (K): by definition, this modality refers to the “perceptual preference related to the use of experience and practice (simulated or real)”. Although such an experience may invoke other modalities, the key is that student is connected to reality, “either through experience, example, practice or simulation”. It is often referred to as “learning by doing”, but that is an oversimplification, especially for college and university learning, which is often abstract but can still be made accessible from those students with a Kinaesthetic preference. This mode is where students use many senses (sight, touch, taste and smell) to take in their environment to experience and learn new things. Some theorists believe that movement is important for this mode but it is the reality of a situation that appeals most.”

The VARK questionnaire comprises 16 multiple choices, of a, b, c, and d. Users can choose more than one answer for each question, and may leave the question blank if they think that it is not applicable.

4.3.3.1 VARK classifications

VARK classification is based on the score obtained from the VARK questionnaire. The scoring and the classification are calculated automatically if the user does the test online. The classifications are explained as below:

a) Uni-modal

If the classification is for only one preference, the person has a uni-modal learning style. Single preferences can be classified into Very Strong, Strong, and Mild. For example, if the person is an Aural preference and scores highly on the aural scale, the person will be classified into Strong Aural. These calculations will be done automatically by the website.

b) Bi-modal

If the classification is for more than one preference, the person has a bi-modal learning styles. The preferences will be one of the following combinations:

VA VR VK AR AK RK

c) Tri-modal

If the classification is for more than two preferences, the person is said to have tri-modal learning styles. The preference would be for one of the following combinations:

VAR VAK VRK ARK

d) Quad-modal

If the classification is for all four modalities, then the person is classified as having quad-modal VARK.

VARK is commonly used, as it is easy, quick and available online at no cost (Rakap, 2010).

4.3.4 Critique about learning styles

There have been critiques made by other researchers about learning styles (Coffield *et al.*, 2004b; Dembo and Howard, 2007). Dembo and Howard (2007) commented that learning styles should not be bothered with, as there is no clear independent empirical evidence to say that learning styles improve student's achievements in the sense of their exam results (such as improve Grade Point Average (GPA)), while criticisms about the advantages of learning styles have been made by few textbooks authors (Coman and Heavers, 1998; Nolting, 2002; Jenkins, 2005; Van Blerkom, 2006). However, the claim only applies in general, regardless of subject or research area. There is evidence in other subject areas that shows a good impacts on students achievements when matched with their learning styles preferences, as compared to those with mismatched styles (Dunn, 1984; Rakap, 2010).

Whilst this research is concerned to improve information security practices, it does not really matter whether there is no empirical evidence about improving student's GPA after applying learning styles. What is most important is that the students show improvements in understanding the subject area in depth (Carver *et al.*, 1999).

4.4 Personalised learning

Given that individuals learn differently, schools are working towards the personalisation of education. Each individual is unique, and has their own preferred learning styles. The learning styles of a person may be influenced by cultural differences (Hayes and Allinson, 1988; Pratt, 1992; Hyland, 1993; Earley and Ang, 2003; Barmeyer, 2004). According to research conducted by Park (1997), Korean, Chinese, and Filipino students were more visual than Anglos. The study also found that in terms of group learning, Vietnamese students demonstrated a major preference, Filipino showed a minor one and Anglo students appeared to have a negative preference. Since these different learning preferences exist, personalised learning is one of the ways to maximise learning experiences. There are two reasons why personalisation is important; first, there are persistent attainment gaps between different groups of pupils such as minority ethnic groups and different genders; second, the world is changing in terms of its diverse society, emergence of technology, competitive knowledge based economy, employer's demands for skilful workers, changing nature in educating and training and the roles of individuals towards environment (Gilbert, 2007). The literature suggested that the term personalised learning originates from Gardner's theory of multiple intelligences (Guldberg, 2004; Johnson, 2004b). The theory suggests that people's interests, needs, abilities and learning styles are important elements in the learning process. Jones and Burns (2006), have defined personalising learning as "the process of tailoring or matching teaching and learning to meet individual needs, interests and aptitudes in order to enable every student to succeed within the education system".

Chapter 4 – Improving the Information Security Awareness and Practices through Education

Another author defined as “tailoring education to individual student need, interest, aptitude or learning preference” (Best, 2007). The term personalised learning may however be ambiguous, and schools and teachers are confused about individualised learning (Courcier, 2007). Courcier (2007) constructed a map (see Figure 26 below) to show the differences in these two terms.

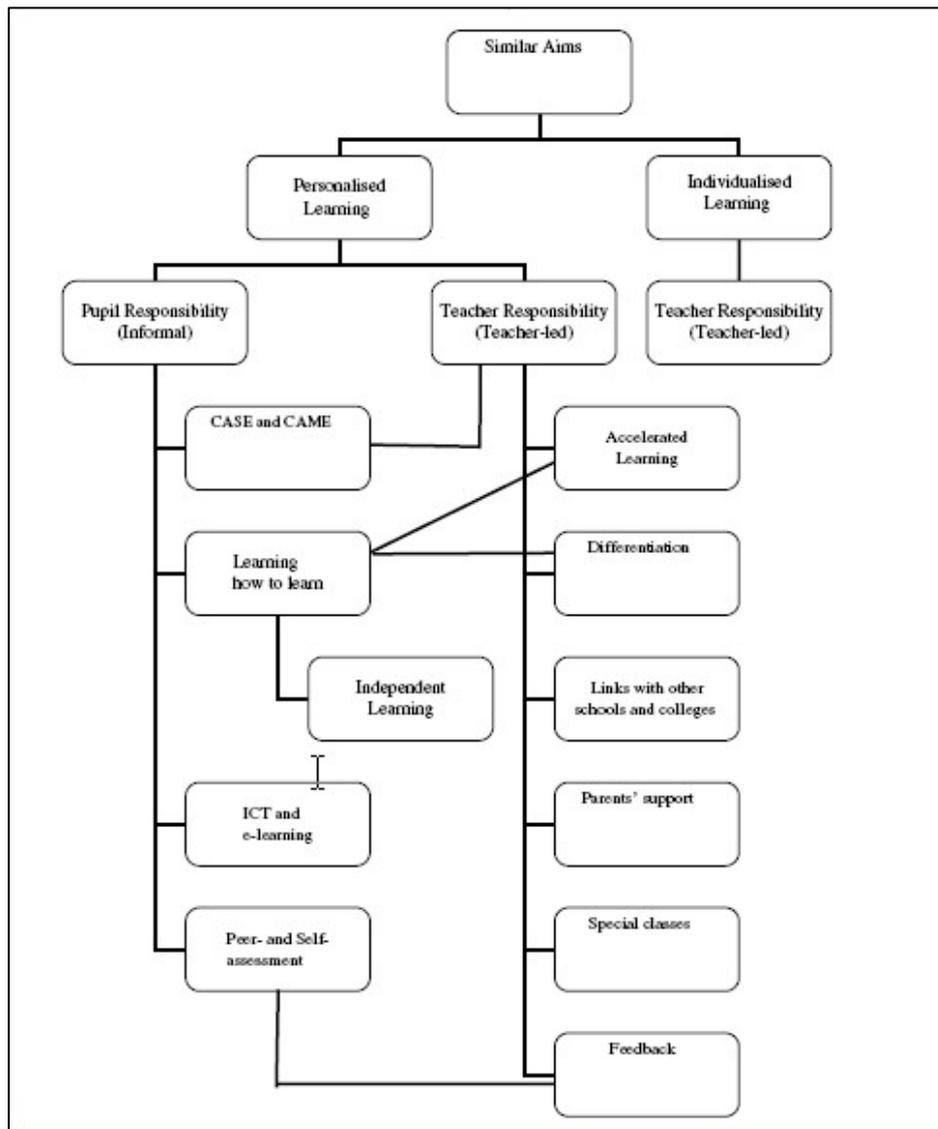


Figure 26 A map showing the links between personalised learning, individualised learning and different approaches

Source: (Courcier, 2007)

Chapter 4 – Improving the Information Security Awareness and Practices through Education

Personalised and individualised learning share the same aims, which are to fulfil individual needs, interests and lifelong learning (Courcier, 2007). However, the differences between both are with regards to the acceptance of responsibilities by the learners and/or teachers. Individualised learning is more about the teacher's responsibilities to help learners towards achieving their goals, as shown in Figure 26. Nonetheless, personalised learning is both teachers and learners' responsibilities to work together in the learning process, as indicated in Figure 26. Personalised learning is different from individualised learning in the sense that it contains elements of individualised learning and one-to-one tuition. The website for the Department for Education (2010) further states that personalised learning "has a strong focus on :

- a) standards, identifying what individual already know, what they need to do to improve and how best they can do so;
- b) pedagogy, developing effective teaching and learning skills through a range of whole class, group and individual teaching;
- c) improving learning and Information Communication Technology (ICT) strategies so as to best transmit knowledge, to instil key learning skills and to accommodate different paces of learning;
- d) inclusion, working to dismantle barriers to learning whatever their causes and to foster the best possible conditions for learning."

Personalised learning at school is about the factors that contribute to the underperforming of pupils. They are individual attitudes, beliefs and expectations of pupils, beliefs and expectations of parents, beliefs and expectations of teachers and social challenges (i.e. urban generations, economic development and migration) (Gilbert, 2007).

Chapter 4 – Improving the Information Security Awareness and Practices through Education

Another author has mentioned learning orientation as the first step to create a personalised learning environment (Martinez, 2002). The author explained the differences in learning orientation and strategies to customise learning in the context of instruction, assessment and the environment. The learning orientations models are described according to four categories: transforming, performing, conforming and resistant learners. Below are the summaries for each of the learning orientations:

- a) Transforming learners (Innovators): described as highly motivated, passionate and highly committed learners. They look at learning as a significant intrinsic resource to make changes in life. In stressful conditions, they rely on their visionary, creative, holistic thinking, sophisticated learning, problem solving and strategic planning ability and the capacity to commit great effort. They are independent, strong, and persistent, determine challenges and exploration, high standards, risk taker, self-motivate in learning. They tend to be bored/frustrated/resistant in environments that mismatch their exploratory and self-directed learning needs. In comparing other learning orientations, they are able to plan well, and strategically execute their important or long term goals. They rely on themselves or prefer mentoring relationships to learn rather than to rely solely on deadlines, structured environments, short-term projects or extrinsic rewards for learning efficacy.
- b) Performing learners (Implementers): described generally as self-motivated in learning situations (task-oriented, project oriented, hands-on applications) that interest them. If they are not interested, they seek extrinsic rewards for accomplishing their objectives. They acknowledge meeting only to perform and complete their objectives and tasks. They are responsible towards their learning but always rely on others for motivation, goal setting, coaching, schedules and directions.

- c) However, they are able to motivate themselves and become successful in situations that very much interest or benefit them. They are detail oriented, lower risk and skilled learners, who are systematic and capable of getting the project done from average to above learning objectives and tasks based on their own personal goals. These learners will lose their motivation if it takes too much effort for them to accomplish a goal and the benefits are not enough to satisfy them. In comparing with other learning orientations, performing learners are short-term, detail and task-oriented. They focus on grades and rewards, take less risk and challenge goals. They are at ease with interpersonal coaching relationships, external support, resources and contacts to complete a task. These learners have more sophisticated skills, as compared to conforming learners.
- d) Conforming Learners (Sustainers): They are passively accept knowledge, store it and produce it to conform and complete their routine or tasks and please others. They like to learn in groups with guidance and feedback. These learners did not typically think holistically, critically, analytically, synthesise feedback, solve complex problems, monitor or review progress independently or accomplish challenging goals. They are less skilled, do not like with decision making and only little desire to control or manage their learning, take risks or initiate changes in their works. They tend to be demotivated in open learning environment that requires focus on high learner control, discovery or exploratory learning, complex problem solving, challenging goals and inferential direction. These learners require scaffolded, structured solutions, guiding direction, simple problems, linear sequencing and explicit feedback. In contrast to other learning orientations, conforming learners are best in well-structured, directive environments and step-by-step procedures. These learners value learning most when it helps them to avoid risk and meet the basic requirement in their job.

Chapter 4 – Improving the Information Security Awareness and Practices through Education

- e) Resistant Learners (Resistance): These learners lack of belief that academic learning and achievement can help them achieve personal goals or make good changes. They always suffer repeated, long-term frustration from improper learning situations. Unfortunate learning experiences or missed opportunity have discouraged these learners from enjoying and using learning to improve them. They also do not believe in formal education and academic institution as enjoyable resources in their life. However, these learners are motivated to learn outside of formal learning institutions. In contrast to other type of learning orientations, these learners are putting their energy to prove that they can progress in informal education.

Learning orientation is general to learning situation and not specified to certain environment. This means that an individual could learn differently based on the situation and environment. For example, a transforming learner might change his/her learning orientation into conforming when the topic is not familiar. However, they will go back to being a transforming learner once they understand the topic. All learning orientations have their own strength and rooms for improvements. They are not being given values to rank each learning orientations to establish which one is better or worst. These learning orientations could be used to alter the method of teaching for example, for transforming learners, the instructor or teacher should give them more independent ways of exploring the subjects or topics. Whilst for conforming learners, the instructor should guide them by giving more structured tasks rather than exploratory. The author also suggests five levels of personalisation strategies. These are:

- a) Name-recognised personalisation – using learners' names when address in learning module.

Chapter 4 – Improving the Information Security Awareness and Practices through Education

- b) Self-described personalisation- learners being asked to answer pre-quiz (or questionnaires, surveys, registration forms and comments) in order to identify their preference, past experiences and existing skills.
- c) Segmented personalisation- using demographics, common attributes, or surveys to groups learning populations for smaller, identifiable and manageable groups.
- d) Cognitive-based personalisation- using cognitive processes, strategies, and the ability to deliver content to specific types of learners. For example, using a diagram and pictures for learners that prefer visual aids.
- e) Whole-person personalisation- using learning orientations (transforming, performing, conforming and resistant learners) to personalised learning materials.

In order to create personalised learning, Paludan (2006) suggests four scenarios:

- a) Total personalisation – personalisation of pupil's route and contents in educational systems.
- b) Personalised timing – personalisation of timing based on different students' journey (such as different ages and adult education).
- c) Automated teaching – using information technology as an alternative to expensive teachers as personalisation needs more teachers' assistance.
- d) Status quo- current situation, namely lack of resources to be invested in educational system and desire to try personalised learning.

Personalised learning is not only being applied in school but also in business applications. Leadbeater (2006) generated three ideas to personalise learning that are based on business applications:

- a) Bespoke service – learning than is tailored to the needs of individual clients/student.
- b) Mass customisation – personalisation within a certain range of standards and modules to suite groups of learner’s goals.
- c) Mass personalisation – customers/learners involve in customising learning modules.

He added more about personalisation to construct a sense of self-actualisation, self-realisation and self-enhancement rather than self-interested with the self-gratification. He also suggested that the personalisation of learning is more suitable for middle class homes where there is space, computers and books.

4.4.1 Challenges in implementing personalising learning

Implementing personalising learning has challenges that need to be resolved. Amongst those challenges, one of them is regarding socio-economic status (Jones and Burns, 2006). Another challenge is to have skilful teachers and teachers’ belief in flexibility in teaching and how to group students (Cutler *et al.*, 2007; Meyer *et al.*, 2008; Mahony and Hextall, 2009). On the contrary, according to a survey, challenges in implementing personalising learning at school are not because of limited experiences or expertise and lack of staff, but due to a lack of finances with multi agency problems and great workloads (National College, 2010). It is clear that resources are the main challenges for implementing personalising learning, as from the previous literature, there is a need for experts and financial resources

In terms of creating learning materials for supporting personalised learning, it is a time consuming process, which teachers need to prepare based on the learners' needs and preferences (Karmeshu *et al.*, 2012; Prain *et al.*, 2012). However, it is worth investing in personalisation as there is evidence of success in implementing it (Prain *et al.*, 2012).

4.4.2 Benefits of personalising learning

Personalising learning encourages teachers to recognise the diversity of their students (Best, 2007). The personalisation agenda is to promote a lifelong learning which not only aims for success in schools and institution but also learning in the future. Researchers agree that personalised learning is an on-going process that promotes deep learning rather than obtaining simple skills and knowledge (Hargreaves, 2006; Leadbeater, 2006). Therefore, it is a good reason to implement personalised learning in educating people about information security, as it should be continuous and not limited to certain skills.

Herlihy & Kemple (2004) reported that the Talent Development Middle School Model in Philadelphia had a positive effect on the implementation of personalised learning for its eight grade (equivalent to Year 7) mathematics. Another encouraging impact on personalised learning is that 11 Boston Pilot Schools managed to raised their standard significantly higher compared to other schools (Center for Collaborative Education, 2006).

The same was also reported by Jenkins and Keefe (2002), where two high schools who implemented personalised learning achieved higher test scores than others in their districts. There is further evidence that personalised learning helps in the learning process:

- 1) The survey of teachers in England undertaken by the National Foundation for Educational Research for the General Teaching Council (Sturman *et al.*, 2005) noted that the aspect of personalised learning most frequently encouraged in schools was

the use of evidence to identify pupils' progress in learning (reported by 90 per cent of teachers in the survey). Other commonly reported factors relevant to personalised learning (reported by over 80 per cent in each case) were being encouraged to get to know pupils well, to offer pastoral care, to accommodate individual learning needs and to give feedback designed to enable pupils to make learning choices.

- 2) In Leadbeater's (2005) *The Shape of Things to Come*, the author draws on visits to six schools and five local authorities to explore approaches to personalised learning. The schools selected were recommended by other schools and local authorities, and appear to be engaging in personalised learning.
- 3) Hargreaves (2006) outlined how pupil voice, assessment for learning and learning to learn can all be seen as contributing to deep learning, consisting of the capacity to learn, control over learning and competencies in contrast to repetition of facts. The curriculum and new technologies enrich the experience of learning, enabling deep learning to be embedded in deep experience and advice, guidance, mentoring and coaching, so as to provide the deep support demanded. This emphasises the fact that personalised learning is not a set of techniques but rather a culture that supports learning process.

4.5 Implementation of the personalised learning

Personalisation of learning has been implemented in primary, secondary and special schools in England (National College, 2008). In primary and secondary school, 'effective teaching and learning' and 'assessment for learning' are the top two strategies to implement personalising learning. The third top strategy for primary school is 'targeted support to overcome barriers to learning' and for secondary school is 'curriculum choice/pathways'. Whilst at special schools, the top three strategies are 'effective teaching and learning',

‘targeted support to overcome barriers to learning’ and ‘a student centred approach to school organisation’ respectively (National College, 2008).

A study conducted in Australian regional low socioeconomic status (SES) schools to investigate the effectiveness of personalised learning (Prain *et al.*, 2012). The investigation found that students in mathematics programme at one of the schools demonstrated improved performance. A further personalised learning implementation in 13 schools in the United Kingdom (UK) was the study conducted by Sebba *et al.* (2007). The study also highlighted that 54% of secondary schools grouped were personalised by ability, 69% of the total schools used open-ended learning challenges and 64% of all school encouraged students to participate in making learning choices.

Personalisation of in the ubiquitous learning system has been proposed by Doherty *et al.* (2006) for courseware entrepreneurial training to individuals working within small and micro-industries. The aim of the personalisation is to be able to deliver learning materials anytime, anywhere. The researchers found that users of the system gave positive feedback after testing it.

4.6 Models of Personalised Learning

The section reviews existing models of personalised learning. These two models were chosen mainly because both use learning styles as one of the elements for personalising learning. These examples are valuable, especially for the development of the framework in the later chapter.

4.6.1 Personalised Collaborative Skills for student Model (CDSM)

This automatic model has been created to analyse students’ personal skills, with the aim of effective collaboration in a distance learning environment (Durán and Amandi, 2009). This

Chapter 4 – Improving the Information Security Awareness and Practices through Education

model has been tested in both a simulated and real environment. The results were very promising, with at least 20% of the students' skill being input for the model to generate which type of user behaviours are. Even though the model was successfully tested and gives good result, the limitation of the model is that it needs a certain amount of input on students' skill to enable it to perform well. The CDSM model consists of three major components; the individual, group and collaboration model:

a) Individual Model

The individual model specifies the background information such as the demographics, background knowledge and personality data (see Figure 27 below). The learning style for this model is Felder and Silverman (Felder and Silverman, 1988). The authors stated that since the target users of the model are Computer Science students, the learning styles is the best the model. However other learning styles may be used. The good thing about the model is that it is flexible in its choices of learning styles, whereby if the intended users were not Computer Science and they wished to use other learning styles, the model would enable this.

The model used personal data and users' previous experiences as a mean of personalising the learning environment. One of the advantages of using users' previous experiences is that the user may save their time from learning the topics that they already familiar with.

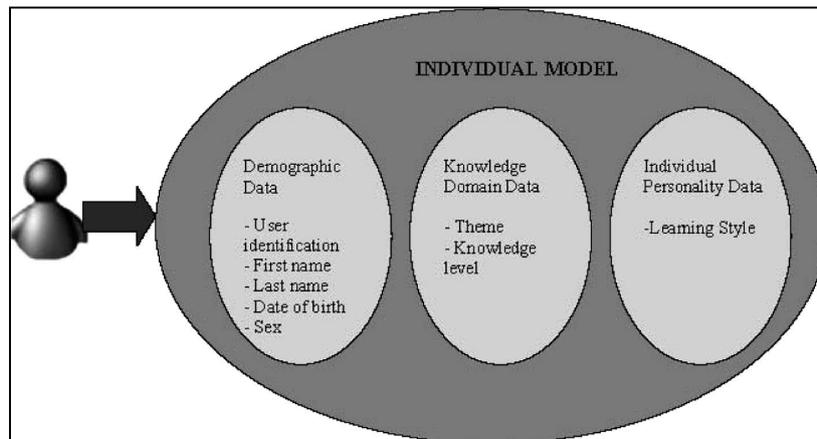


Figure 27 Individual model

Source: (Durán and Amandi, 2009)

b) Group Model

The group model was intended to group students based on their personal behaviour. The elements of the group identification are: type of group, conflict, contract, division of work and roles (see Figure 28 below). These features enable students to know if they are suitable for working with others, by indicating that they may work with others or not. These students may be grouped based on their preferences. Group members could be gathered in balance with the feature of 'roles'. For example, if the role of the student is as leader, then, the model selects group members where there is only one leader in the group. This group model was created to take into account of individual elements (such as individual learning preference and personality) in a group-based learning environment.

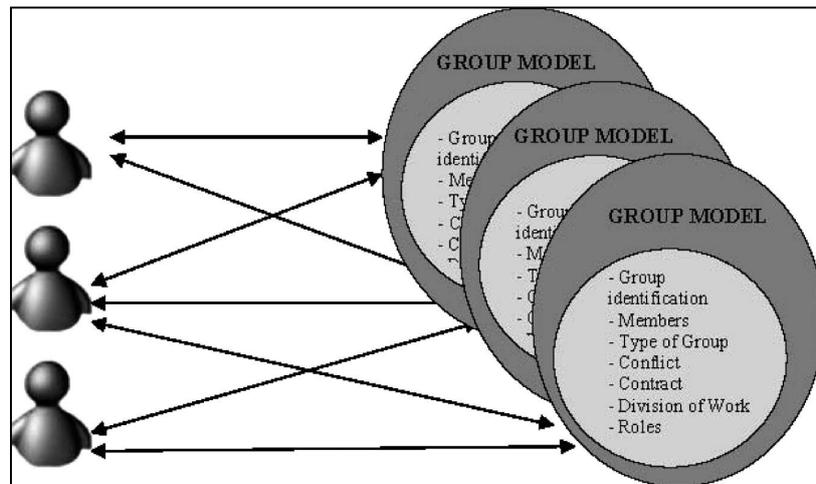


Figure 28 Group model

Source: (Durán and Amandi, 2009)

c) Collaborative model

The collaborative model (see Figure 29) takes into account other factors that affect students behaviour, for example the situation. This model combines the other two models to form a dynamic learning environment. For example, a person will behave in certain ways according to the situation.

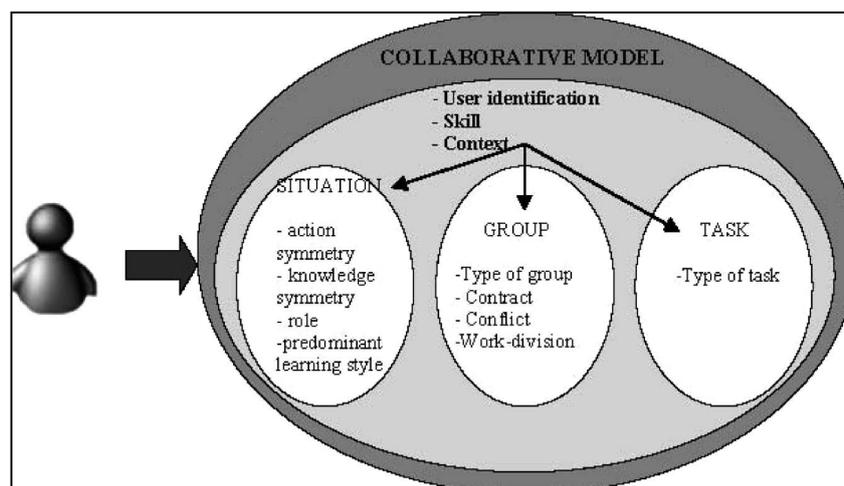


Figure 29 Collaborative model

Source: (Durán and Amandi, 2009)

The element of personalising learning styles helps individuals to learn better because they learn according to their own preferences. These three models are good in terms of providing

an analysis of students' behaviour. The limitation of the model is that it can only assess students' behaviour if the system knows at least 20% of the students' skills.

4.6.2 Conceptual model for construction

A conceptual model for personalised learning environments (PLE) prototype that integrates learning styles was developed for the United Kingdom construction industry (Syed-Khuzzan and Goulding, 2009). Syed-Khuzzan and Goulding (2009) used a qualitative approach in the study. This model (see Figure 30 below) is using three types of learning styles model; Kolb's model (Kolb, 1984), Honey and Mumford's model (Honey and Mumford, 2006), and Felder and Silverman Model (Felder and Silverman, 1988). The authors chose these models because they were the most cited and used in a web-based learning environment, and also successfully implemented in a traditional classroom context. A diagnostic questionnaire was created in order to group users into learning styles. The three learning styles models were analysed to determine the overlapping styles. Then these styles were grouped into four styles A, B, C, and D (see Figure 30). Each of the learning styles has a set of questions that may determine how the user fits into the learning styles' classification.

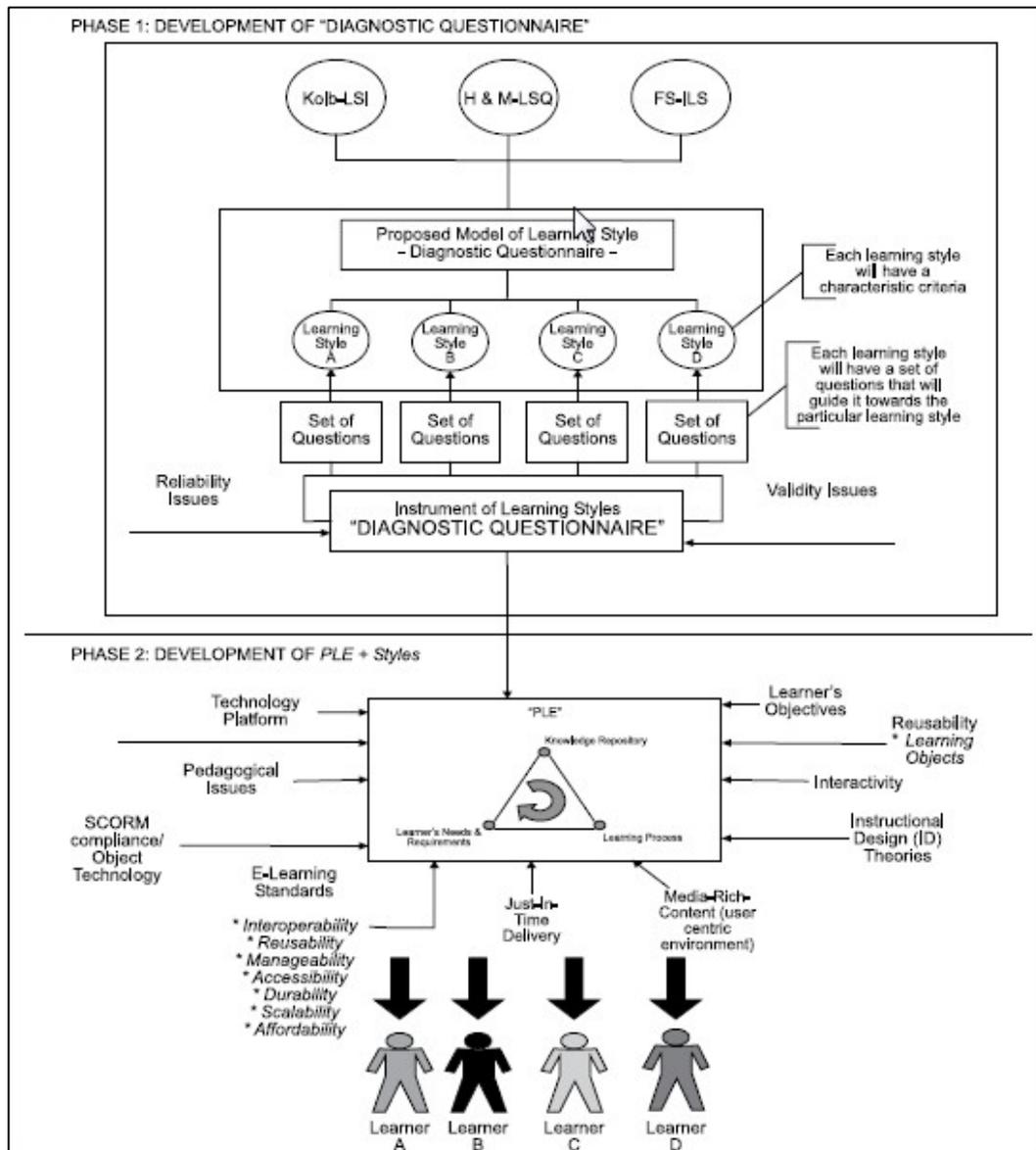


Figure 30 PLE Prototype incorporating learning styles conceptual model

Source: (Syed-Khuzzan and Goulding, 2009)

This paper contributes examples on how to develop personalised learning environments that integrate with learning styles. The authors highlighted the importance of incorporating learning styles into the PLE:

- a) Individual might be dominated by one and some might be more or combination of learning styles.
- b) From the literature, (Kolb, 1984; Sims, 1990; Kim and Chris, 2001) demonstrated that learning can be enhanced by incorporating various learning styles in the instructional process
- c) Learning should be personalised and 'one size fits all' approach is ineffective (Vincent and Ross, 2001b; Watson and Hardaker, 2005).
- d) Alsubaie, (2006) suggested that learning styles should be incorporated in a learning environment to achieve a holistic environment that appeals to a whole raft of learners.

The idea of using the three learning styles is good in order to avoid overlapping of the learning preferences. However, the diagnostic questionnaire that is used to group people according to their learning styles would be time consuming because the user has to answer the three different learning styles test. This model only provide a platform of tailoring learner's preferences but not taking into account of collaborative learning environment such as giving learners opportunity to share their pre-existed knowledge and opinions. Overall, the model is a good example for creating a personalised learning environment.

4.6.3 Personalised learning system based on Solomon Learning Style

This system is good not only for learners, but also teachers who are interested in educating non-university education (Liu and Chen, 2008). Since information security education may be categorised as non-academic (non-cognitive and persuasive), it is worth considering the implementation of the personalised learning in the area (Siponen, 2000).

The result of the experiment shows that the system is able to establish a personalised learning environment, which the author believes could improve the efficiency of the learning.

Chapter 4 – Improving the Information Security Awareness and Practices through Education

The system is able to identify learners' learning preferences by analysing previous learners' records if they did not do the learning styles test. There is flexibility in terms of having assessment as part of the learning materials, with learners being able to do the test at the beginning, middle or end of the learning process. The test questions exist in three level of difficulty; difficult, moderate and easy. The structure of the personalised learning is presented in the Figure 31 below:

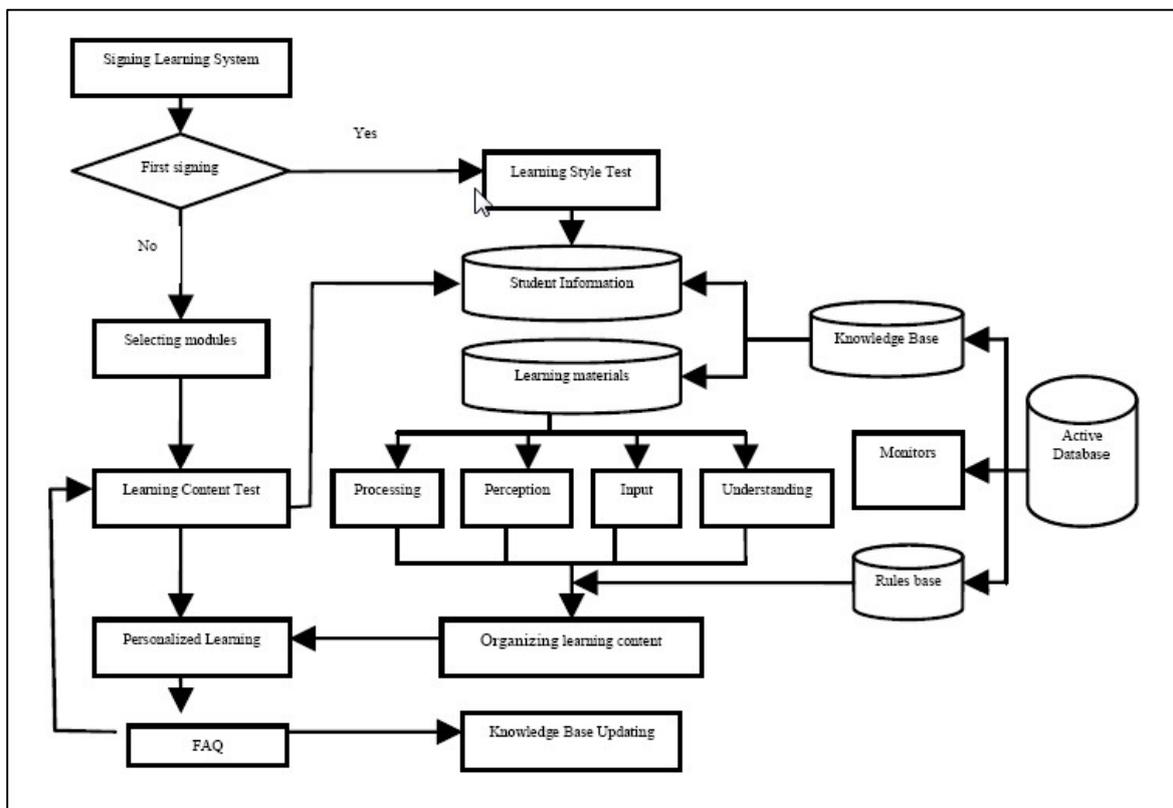


Figure 31 Structure of personalised learning system - Solomon's Learning styles based

Source: (Liu and Chen, 2008)

The disadvantage of this model is that it only implements one type learning style Solomons' Learning Styles as a fixed learning styles test. Only teachers could uploaded the contents whereas, personalising education should include learners' feedbacks and experiences (Courcier, 2007). The experiment only proved the ability of the system to create personalised learning environment, but not mentioning on the performance of the learners who has been using the system

4.7 Conclusion

From the above reviewed information security awareness and pedagogy, the four pedagogical approach suggested by Karjalainen and Siponen, and the conceptual change approach by Yuen-Yan and Wei may be adopted to enhance information security awareness education (Yuen-Yan and Wei, 2009; Karjalainen and Siponen, 2011). Both suggested approaches are missing the personalised learning element, which is widely used in educational areas. The advantages of personalised learning have been discussed in the previous sections, where previous studies show that there are improvements in students' performance at school and in industries. Moreover, the collaborative student model reviewed in this chapter also provides good results for having personalised learning feature. One of the methods of personalisation is to pay attention to people's learning styles. Learning styles as used in the school and adult education examples were presented in the earlier sections.

In summary, information security awareness may be improved by using a pedagogical approach via personalising information security education using learning styles. VARK learning styles have been chosen for the later study on the usefulness of learning styles in teaching information security topics.

5 An Investigation into Improving Information Security Practices through Personalised Learning

5.1 Introduction

Given the need to establish more effective information security education and the success that personalised learning has had within the primary/secondary education domains, it seemed prudent to understand and evaluate the effectiveness that such an approach could have within the domain of security education. A study has therefore been conducted to investigate whether using a learning styles approach may serve to enhance the learning process in the information security area.

5.2 Methodology

5.2.1 Research design

To investigate the usefulness of learning styles for teaching information security, the learning styles of the participants should be determined. In order to do so, at the beginning, the participants needed to complete learning styles test. This was to determine which learning styles that the participants had. So as to assess the learner's performance, the researcher chose to have pre and post-tests in order to compare learners' scores. The purpose of the pre-test was to ascertain whether there was any pre-existing knowledge of the participant on the topic in learning materials (later, the participants would be given four information security sub-topics to be learnt). The post-test, meanwhile, was created to assess the understanding of the participants on the learning materials given. In between the tests, the participants learned about information security topics that had been prepared by the researcher, which were presented in four different ways, representing four different learning styles (VARK).

Chapter 5 – The Study of Improving Information Security Practices

In addition to this, user experience survey and demographics information were needed for further information as to who the participants were, and their feedbacks. For the above reasons, the study was designed to cover five parts:

- Part 1, learning styles questionnaire;
- Part 2, pre-test questions;
- Part 3, learning materials;
- Part 4, user experience survey which includes demographic questions;
- Part 5, post-test questions.

In Part 1, Visual, Aural, Reading/writing and Kinaesthetic (VARK) questionnaire version 7.1 from the VARK websites developed by (Fleming, 2001).

Part 2 was the pre-test intended to acquire information about participants' prior knowledge on the learning material being given in the Part 3. The study used pre and post-tests as they were one of the most simple methods for testing the effectiveness of learning materials (Shuttleworth, 2009). The test was designed with 24 multiple-choice questions (MCQs) in total, and five choices of answers. The total number of questions was designated so that each types of learning style would have six questions. If the researcher had used more questions, this may have added more time to the study session. Question 1-6 were about learning materials presented in Reading learning styles, Question 7-12 were about the materials in Aural learning styles presentation, Questions 13-18 were for Kinaesthetic learning styles and Questions 19-24 were about Visual learning styles materials. The questions for each type of learning materials were made invisible to the participants, so as to avoid bias when answering the questions.

Chapter 5 – The Study of Improving Information Security Practices

Part 3 comprised the learning materials created around the four different styles of learning. Topics I, II, III and IV represented Visual, Aural, Reading/writing and Kinaesthetic learning styles respectively.

Part 4 was created to elicit participants' opinion on their experiences, and to distract them from thinking about the learning materials before they proceeded to the next session.

Part 5 was the post-test, where the participants answered the same set of MCQs as in the pre-test. The test was also intended to understand if the participants learned better with the materials that matched their learning styles. A summary of the whole process of the study session is provided in Figure 32 below:

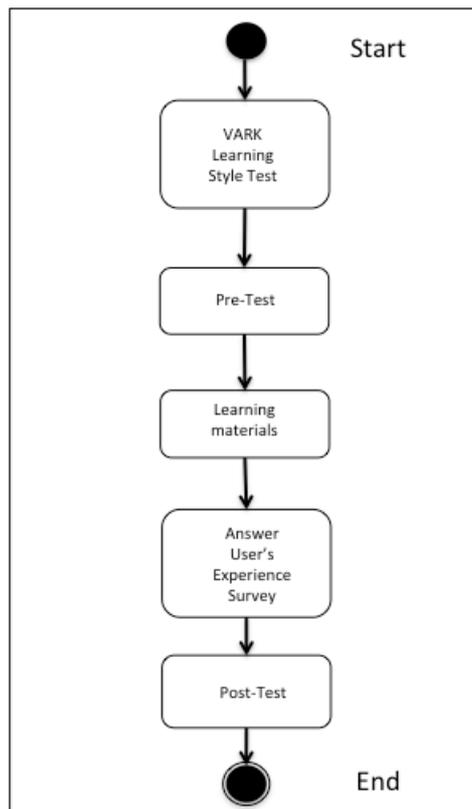


Figure 32 Summary of study session

5.2.1.1 VARK learning styles questionnaire

Alexandra and Georgeta (2011) found that identifying students' learning styles facilitate the learning process, and it is important to have different types of learning materials and helping student with their learning preferences. VARK was chosen out of others because it is a commonly used learning styles inventory, and available free via the VARK website (French *et al.*, 2007; Wehrwein *et al.*, 2007; Kalkan, 2008; McKean *et al.*, 2009; Meehan-Andrews, 2009; Rakap, 2010; Koch *et al.*, 2011). The participants and the researcher were able to access the VARK test easily from the Web as long as they have an Internet connection. Even though there is a hard copy version of the VARK questionnaires, the researcher chose to use the online version, as it would automatically calculate the VARK results and classify the participant into their learning preferences. Moreover, it is a quick, simple, convenient and concise 16 items questionnaire to be completed by the participants (Murphy *et al.*, 2004; Alkhasawneh *et al.*, 2008; James *et al.*, 2011). In terms of validity of the VARK test, Bonwell and Hurd (1998) found there were significant correlations between the learning strategies that students adopt and their VARK classification from the test. Furthermore, Leite *et al.* (2010) also provide evidence on the validity of the test in their research. Based on the above reasons, the study chose to use VARK for assessing participants' learning styles.

5.2.1.2 Learning materials

Topics in the learning materials were based on the general biometric. The topic was selected as it is one of the information security topics that not considered as excessively technical and accessible to the public. For example, biometric was chosen rather than passwords because the public would be more familiar with the topic as they are using password regularly and would have a pre-existing level of education about it. The reason why the study needed such an unknown topic was that the participants were supposed to learn the topic from the materials being presented to them to assess the effectiveness of using the learning styles approach in improving learning process. If a participant were to be able to

Chapter 5 – The Study of Improving Information Security Practices

score highly on the pre-test given pre-existing knowledge of the topic, this would reduce the ability to measure the usefulness of the learning approaches.

Initially, the researcher considered creating the same topic and presenting it in four different ways. For example, the subtopic 'biometrics performance' would be presented in Visual, Aural, Read/write and Kinaesthetic styles. However, if the participants had gone through all four styles each time, this would have been a repetitive process. Moreover, it would have been difficult to measure participant's performance, as they would have experienced the same topic four times.

After considering the time constraint, the researcher decided to use another approach. Four small topics from Biometrics were created in four different learning styles to suit the visual, aural, read/write and kinaesthetic learners. It was designed and arranged in such way that each session would contain about five minutes of learning materials. This was done so to avoid tiredness and ensure the experiment in its entirety did not last more than 1 hour. For example, after the visual topic, the participant was asked to listen to a short lecture for five minutes; then read a long text for read/write materials; finally, the fourth topic was a short five minutes video representing kinaesthetic learner's materials.

All four topics were created based on the suggestions from one of Fleming's book entitled Teaching and Learning Styles: VARK strategies (Fleming, 2006). For visual topic (General Biometric Authentication), the researcher used diagram, coloured diagrams, underlining important words, highlighting subtopics, used symbols such as "→", "+" and "=" symbols. Aural topic (User Acceptance) was a short text being read by a native English speaker and recorded as an audio file. Two readers were invited to read the text; one was a native speaker, and the other was an international student.

The English reader was chosen based on his clear pronunciations and ability to deliver the short lecture in a five minutes period. The strategy used for the Aural topic was a 'hearing' method (as described in Flemming's book which refers to listen method), with the participant being able to replay the lecture if they felt it was necessary. The third topic, Read/write (The State of the Art in Biometric Performance) was created using lists and definitions strategies. The final topic for Kinaesthetic (Modalities) was to use a short video, and the strategies adopted were real learning experiences, real photographs and real-life examples.

5.2.1.3 User experience survey

The survey was intended to elicit participants' preferences in terms of the learning process. In this part, moreover, demographic information was asked of the participants. Questionnaires were used in order to collect the information regarding the study. This method had its advantages, in that it is quick to collect information from people (Sociology.org, 2012). Another reason why questionnaires were used was the anonymity of the survey technique, which enabled the respondents to give honest answers (Milne, 1999).

5.2.2 Preliminary study report 1

The purpose of the preliminary study was to test the viability of the learning materials, the methods and to estimate the amount of time taken by a participant to complete each study session. A male participant holding a Bachelor degree in Human Sciences who did not have a formal education regarding Biometrics was the first participant in the study. The participant was chosen with the hope that the person had learned from the study, and the usefulness of the learning materials itself could be tested. Below are the materials being used in the study session:

- 1- Pre and post-test questions - Hardcopies of the test
- 2- A laptop – softcopy of the learning materials
- 3- An earphone

Chapter 5 – The Study of Improving Information Security Practices

The combinations of hard and soft copy were used to avoid eye strain for participants during the study session. An earphone was used for a better hearing experience, as the session required participants to focus and understand the short lecture and the video.

Pre and post-tests consisted of 24 MCQs, chosen so that each learning style would have six questions. The study consisted of four parts, as below:

- a) Part1: Pre-test where the participant was required to answer 24 multiple-choice questions (MCQs) from the four subtopics of biometric. Refer to Appendix E for the pre-test question
- b) Part 2: Learning materials where the participant was taught about Biometric topics in four different ways. Refer to Appendix F for the learning materials.
- c) Part 3: VARK questionnaire where the participant answered the 16 MCQs to assess their learning styles. This questionnaire was completed online via the VARK website (Fleming, 2001). The printed version of the VARK questionnaire could be found in Appendix K.
- d) Part 4: Post-test where the participant was required to answer the same set of questions as in pre-test.

The time taken for the participant was recorded in order to estimate how long a participant would finish the study session. Overall time taken by the participant in the study was nearly an hour.

Chapter 5 – The Study of Improving Information Security Practices

The breakdown of the time taken for each part of the experiment is presented in the Table 22 below:

Table 22 Time taken to complete the experiment

Part	Time taken by the participant to complete
Pre-test	11 minutes 53 seconds
Materials	Visual – 12 minutes 53 seconds Aural – 4 minutes 14 seconds Reading – 4 minutes 52 seconds Kinaesthetic- 5 minutes 44 seconds Total material section: 27 minutes 43 seconds
VARK questionnaire	6 minutes 14 seconds
Post-test	9 minutes 22 seconds
TOTAL EXPERIMENT TIME	55 minutes 12 seconds

The table below (see Table 23) demonstrates the summary results of Pre and Post-test for this study:

Table 23 Preliminary study: Comparisons of the pre and post-test results

Topic	Learning Styles	VARK Score	Question No.	Pre-test	Post-test
Performance	Reading and Writing	12	1	0	1
			2	0	0
			3	0	0
			4	1	0
			5	1	1
			6	1	0
			TOTAL	3	2
User acceptance	Aural	8	7	1	1
			8	1	1
			9	0	0
			10	0	1
			11	1	1
			12	0	0
			TOTAL	3	4
Modalities	Kinaesthetic	9	13	1	1
			14	1	1
			15	1	1
			16	0	1
			17	0	0
			18	0	1
			TOTAL	3	5
Technical	Visual	9	19	0	1
			20	1	1
			21	1	1
			22	0	0
			23	1	1
			24	0	1
			TOTAL	3	5

The participant has a multimodal approach to learning styles. He scored the highest for Reading/writing, followed by Kinaesthetic, Technical and Aural. He improved the test scores in post-test for all the questions presented in all four different learning styles except for Reading/writing section, which was expected to score more as he scored the highest in the Reading/writing VARK learning styles test. However, this test was conducted to one person where, it could be a unique case for the person where learning styles would not be the factor that influenced his learning performance. Overall, his score improved in the post-test. This shows that the learning materials in the study are useful and effective in teaching people about the particular topic. Hence, the second preliminary study has been conducted with the assumption that there were positive results from more people in the study.

5.2.3 Preliminary study report 2

In the second preliminary study, changes were made to improve the study. For example:

- 1) Questions in pre-test and post-test that were too dependent on the learning materials were changed into a more general question, as below:

“Q5: In the UK Passport Service study, which process takes longer to complete?

- a) Enrolment
- b) Verification
- c) Screening
- d) Transmission”

Replaced with:

“Q5: The following factors below should be considered when developing and implementing a biometric system **except**: (Choose only one answer)

- a) Time needed to enrol users’ biometric characteristics
- b) Individual disabilities during the enrolment process
- c) Users’ computer skills

Chapter 5 – The Study of Improving Information Security Practices

- d) Users' training programme
- e) Privacy issues relating to system security".

Question 8 was removed and a new question added:

"Q8: According to a research conducted at George Washington University, the respondents prefer to use biometric technology for:

- a) Commercial, banking institution, travel and medical procedures
- b) Office physical access, air transportation screening, medical procedures and government functions
- c) Financial institution, medical procedures, commercial and government functions
- d) Banking institution, transportation screening, medical procedures and school"

Replaced with:

"Q8: What are people's concerns when using a biometrics system? (Choose only one answer)

- a) Loss of fingers and biometrics data
- b) Their movements are tracked and misused by government
- c) System is not user friendly and being framed for crime scenes
- d) a and c only
- e) a, b and c only"

2) All answer options were increased from four (a,b, c, d) to five with additional 'e' in the pre and post-tests. The more options participant had, the more chances of them to show their knowledge and understanding of the materials (Diehl and Doucette, 1999).

Chapter 5 – The Study of Improving Information Security Practices

Three participants were invited to take part in the second study. These participants were selected based on their diverse educational backgrounds, covering Electrical and Electronic Engineering, Marine Sciences and Medicine respectively. They became good participants, as they did not have formal exposure to Biometrics topics in the learning material. Table 24 shows the information of the participants:

Table 24 Participants' information

User	Gender	Education
2	Male	College
3	Female	Undergraduate
4	Male	College

See Table 25 below. These are the materials required and being used in the study. The experiment consists of five parts as below:

- a) Part 1: Learning styles questionnaire - Participant were asked via email to complete the VARK questionnaire prior to the experiment. The questionnaire consisted of 16 MCQs to assess their learning styles. The questionnaire were completed, online at the VARK website and email their result to the researcher (Fleming, 2001)
- b) Part 2: Pre-test Questions – the updated version of the pre-test questions are in Appendix H. and the answer key to the test is in the Appendix I.
- c) Part 3: Learning materials
- d) Part 4: User Experience Survey - the participants were asked on information about them and their learning experience on the materials provided. A copy of the survey is attached in Appendix L
- e) Part 5: Post-test Questions

Table 25 The materials used in the study

Materials
1) Hardcopy of: a- Pre-test questions b- User experience survey c- Post-test questions
2) Laptop / Desktop for presenting the learning materials
3) An earphone for listening to the Aural and Kinaesthetic learning materials

There were changes in the study session parts where in this study, Part 1 were completed prior to the experiment session (to save time) instead of the pre-test in the first study. Another change was the additional Part 4 (User Experience Survey) being included to acquire demographic, and participants' experience information during the study session

5.2.3.1 Result

The table below (refer Table 26) shows the breakdown of time taken for users to complete the experiment.

Table 26 Time taken by participants to complete the second preliminary study

Part	User 2	User 3	User 4
Part 1 - Learning Styles Questionnaire (VARK)	6 : 20	5 : 00	3:48
Part 2 - Pre- test	18 : 10	21 : 13	17:29
Part 3 – Learning Materials			
Topic I Technical (Visual)	6 : 55	7 : 01	18:18
Topic II User Acceptance(Aural)	5 : 17	5 : 00	5:00
Topic III Performance (Reading/Writing)	7 : 13	5 : 42	5:53
Topic IV Modalities (Kinaesthetic)	6 : 28	5 : 29	4:28
Part 4 – User experience survey	3 : 20	4 : 46	2:39
Part 5 – Post –test	10 : 59	8 : 37	10:28
TOTAL EXPERIMENT TIME	64 : 42	62 : 48	68:03

All three participants took within one hour and nine minutes to finish the session. The Table 27 shows the results for the second preliminary test:

Chapter 5 – The Study of Improving Information Security Practices

Table 27 Results for the second preliminary study

		User 2			User 3			User 4			
Learning Styles	Question No.	Pre-test	Post-test	VARK Score	Pre-test	Post-test	VARK Score	Pre-test	Post-test	VARK Score	
Reading and Writing	1	0	0	12	0	0	6	0	0	5	
	2	0	0		0	1		0	1		
	3	0	1		0	1		0	1		
	4	0	0		0	0		1	1		1
	5	0	0		0	1		0	0		
	6	1	1		0	0		1	1		
	TOTAL	1	2		0	3		2	4		
Aural	7	0	0	5	0	0	3	0	1	4	
	8	0	1		1	1		0	1		
	9	1	1		0	0		0	1		
	10	0	1		1	1		0	0		
	11	0	1		0	1		1	0		
	12	0	0		1	0		0	1		
	TOTAL	1	4		3	3		1	4		
Kinaesthetic	13	1	1	3	1	1	4	0	1	7	
	14	1	1		0	0		1	1		
	15	1	1		1	0		0	1		
	16	1	1		0	1		0	1		
	17	0	0		0	1		0	1		
	18	0	1		0	1		0	1		
	TOTAL	4	5		2	4		1	6		
Visual	19	1	0	7	1	0	3	1	0	0	
	20	0	1		0	0		0	0		
	21	1	1		1	1		1	1		
	22	0	0		1	1		0	1		
	23	0	1		0	0		0	0		
	24	0	0		0	0		1	0		
	TOTAL	2	3		3	2		3	2		

5.2.3.2 Discussion

Most of the participants had a multimodal learning style. However, User 3 had a mild reading/writing style, as defined by the author of VARK, and User 4 had a zero score for visual style. Overall, all of the participants showed improvements in their post-test, compared to the pre-test scores. This again demonstrates the usefulness of the learning materials of the study.

User 1 and 2 had high scores in reading/writing style in the VARK test. User 1 did not improve, but decreased by 1 mark in the post-test questions for reading/writing, while user 2 improved his score by 1 mark in the post-test in the reading/writing questions. Based on the VARK score, both of the users should score more in the reading/writing than the other sets of questions for aural, visual and kinaesthetic.

User 3 had the highest score in reading/writing in the VARK learning styles test. It is interesting to note that the user also improved most in her post-test for the reading/writing questions. User 4 had a zero score on visual styles in the VARK test. However he did not improve on his post-test for the visual questions. This indicates that learning styles had an impact on user 4, as he did not perform well in the section that he did not like (in this case, the visual section).

5.3 Study on the effectiveness of learning styles upon learning information security topic (Main study).

After gaining approval from the Faculty of Science and Technology Human Research Ethics Committees, Plymouth University, the experiment was advertised in the Plymouth University staff and students' portal as a paid experiment to motivate participants, as the study took almost an hour to be completed for each session (Refer to Appendix J for the approval application form).

Chapter 5 – The Study of Improving Information Security Practices

The appropriate respondents for the study were individuals without formal education in information security. This is because it was expected that they would learn about the topic from the learning materials prepared for them, not from their pre-existing knowledge. Forty participants were chosen as a sample size. This was considered sufficient insofar as other research which had been conducted using the same sample size achieved a meaningful analysis. (Diehl, 2004; Swaak, 2009) Each participant received an amount of £10 upon completing the study session, in order to provide an incentive to participate. The participants needed to come to the researcher's office for the experiment session. Each participant was given a consent form with details of research information.

After the participants read and understood the procedure, they printed their signatures in the forms given as an indication of their agreement to participate in the study. The procedures for each experiment session were as follows:

1. The researcher gave the research information sheet to a participant to give them ideas on what they had to do in the study.
2. Once the participant was ready, he/she used a laptop provided by the researcher and started with Part I: Learning Styles VARK questionnaire. The participant completed the questionnaire online, and upon completion, the researcher recorded the results in a secured database in the laptop.
3. In Part II: Pre-test, the researcher gave a hardcopy of the pre-test, which consisted of 24 multiple-choice questions (MCQs) to be completed.
4. The participant was given a three minutes break before continuing to the next part.
5. In Part III: Learning materials, the participant went through the learning materials in the laptop. He/she read texts and diagrams, listened to a short lecture and watched a video in the session.

6. Part IV: User experience survey, a participant was given a short survey consisted of 6 MCQs to share their thoughts and experiences on the learning materials as well as some of the demographic information.
7. Finally, Part V: Post-test, respondent was given a hardcopy of 24 MCQs to be completed to assess what they have learnt from the learning materials.

Questionnaires were used to collect the information regarding the study. This method had the advantage of being quick to collect information from people. Another reason why questionnaire were used in the study was the anonymity of the survey technique, which encouraged respondents to give honest answers.

5.4 Results

5.4.1 Demographics

The result shows 23% out of the total 40 respondents were male, and the rest were female participants. As the study was focused on how people learnt instead of gender, it is considered as an appropriate sample of participants for the study. In referring to Table 28, the majority of the participants' learning preferences were VARK. This is normal; as compared with the statistics from the VARK websites where 35%² of the participants who made VARK test online turned to be the highest percentage amongst the other learning preferences (see Figure 33). Fleming (2011b), stated that people lives in a multimodal environment, and this is the reason why the majority of them prefer VARK as their learning style. Therefore, it was anticipated that VARK would be seen as popular amongst the participants.

² The data is based on the VARK database October-December 2011.

Chapter 5 – The Study of Improving Information Security Practices

70% of the total participants at least held a bachelor's degree, and another 30% were colleges and school graduates. This is because the majority of the participants were Plymouth University's students and staff. Since the objective of the study was not to target any specific level of education, the sample of participants was intended to represent the intended respondents.

In terms of single preferences, 10% out of the total participants chose Aural (A) and Read/write (R) (each) and 3% for Kinaesthetic (K) and none for Visual (V). This finding was similar to the VARK statistics in the sense that both results have R as the highest and lowest percentage for V. This information could be obtained from the Table 28 and Figure 33. Read/write learning style is popular because people read for leisure, and make it their habit (Clark and Rumbold, 2006; Karim and Hasan, 2007).

Table 28 VARK classifications and gender

Classification	Gender		Total
	Male	Female	
A	0	1	1
MILD A	0	2	2
STRONG A	0	1	1
MILD R	0	3	3
STRONG R	0	1	1
MILD K	1	0	1
AR	0	1	1
VR	0	2	2
VA	0	1	1
VRK	0	4	4
VAK	0	3	3
VARK	8	12	20
Total	9	31	40

Profile	Total %	mild	strong	very strong	Category	Category %
V	3.0	2.1	0.6	0.3		
A	7.7	5.3	1.7	0.7		
R	15.4	8.2	4.0	2.3		
K	12.2	7.5	3.2	1.5		
					Single preference	38.4
VA	0.6					
VR	1.1					
VK	2.5					
AR	3.3					
AK	4.7					
RK	3.2					
					Bi modal	15.3
VAR	0.8					
VAK	3.0					
ARK	6.2					
VRK	2.2					
					Tri modal	12.2
VARK	35.4					34.1
Total	100%					100%

Figure 33 Table for VARK database October-December 2011: Distribution of preferences

*Source: (Fleming, 2011b)

5.4.2 Analysis based on VARK classification

The study was designed with the intention of ascertaining whether learning style (VARK) helps people with the learning process. The assumptions made by the researcher were as follows:

- a) Participant who scored highly in the Visual learning style in the VARK test would have positive and better score for Visual Improvement score (V-IS) as compared to the other three learning styles. V-IS is calculated by subtracting the visual post-test score from the visual pre-test score.
- b) Participants who scored highly for Aural learning style in the VARK test would have a positive and better Aural Improvement score (A-IS). A-IS is calculated by subtracting the aural post-test score from the aural pre-test score.

- c) Participants who scored highly in the Read/write learning style in VARK test would have a positive and better score for Read/write Improvement score (R-IS). R-IS is calculated by subtracting the read/write post-test score from the read/write pre-test score.
- d) Participants who scored high in Kinaesthetic learning style in VARK test would have positive and better score for Kinaesthetic Improvement score (K-IS). K-IS is calculated by subtracting the kinaesthetic post-test score from the kinaesthetic pre-test score.
- e) Participant who scored low for Visual learning style in VARK test would have a negative and low score for V-IS.
- f) Participant who scored low for Aural learning style in VARK test would have a negative and low score for A-IS.
- g) Participant who scored low for Read/write learning style in VARK test would have a negative and low score for R-IS.
- h) Participant who scored low for Kinaesthetic learning style in VARK test would have a negative and low score for K-IS.

5.4.2.1 Uni-modal Aural (A)

Four of the 40 participants who were identified as A-type persons. Below are the detail scores for A persons:

Table 29 Detailed scores for Aural participants

ID	VARK Scores				Improvement Scores				Classification
	V	A	R	K	V-IS ³	A-IS ⁴	R-IS ⁵	K-IS ⁶	
22	0	9	5	2	0	2	-2	0	A
23	9	14	6	9	1	0	0	3	Mild A
33	8	15	2	10	1	3	-2	3	Mild A
11	2	8	2	4	1	3	1	2	Strong A

³ V-IS stands for Visual Improvement Score

⁴ A-IS stands for Aural Improvement Score

⁵ R-IS stands for Read/Write Improvement Score

⁶ K-IS stands for Kinaesthetic Improvement Score

Three of the four participants with ‘A’ classification, regardless of whether it was a mild or strong A, scored the highest improvement score in the aural section. This satisfies the assumption (b) in the previous subsection whereby the participants scored better for A-IS. The result also indicates that ‘A’ people would learn better using materials presented for ‘A’ learning styles. In referring to Table 29 above, two of the four participants scored the highest in their kinaesthetic section. This may be because the short video for kinaesthetic learning materials involved a listening task which was their preference. The results also demonstrate that the condition of unmatched learning styles leads to lower improvement scores in the Visual and Read/write section.

5.4.2.2 Uni-modal Read/write (R)

There were four participants who were recognised as R uni-modal (refer to Table 30). Three of them were Mild R and another was Strong R. The participant with the strong R had the second highest improvement score for the reading section. It is expected that these participants should score the highest for R-IS. However, none of them scored the highest for R-IS. Even though there was no highest R-IS by these four participants, the result shows that only one of them scored the lowest. Two out of four scored the highest in K-IS.

Table 30 Detailed scores of uni-modal Read/write participants

ID	VARK Score				Improvement Score				Classification
	V	A	R	K	V-IS	A-IS	R-IS	K-IS	
12	3	4	8	5	0	-1	1	4	Mild R
30	1	4	7	4	0	1	0	2	Mild R
39	2	5	7	2	-3	2	0	1	Mild R
36	9	4	16	7	3	0	2	2	Strong R

5.4.2.3 Uni-modal Kinaesthetic (K)

Only one of the total participants had a K learning styles and scored the highest for K-IS. The results show that this person learned best with K material. The person also scored ‘0’ for visual, and this was defined as ‘void on V’ by the author of VARK (Fleming, 2006).

Chapter 5 – The Study of Improving Information Security Practices

The V-IS for the person was negative which it reflects his unfavourable preference towards V materials. This information is presented in Table 31 below. However, since only one person that turned out to be a K person, further comparison could not be undertaken for uni-modal K.

Table 31 Detailed scores of uni-modal Kinaesthetic participant

ID	VARK Score				Improvement Score				Classification
	V	A	R	K	V-IS	A-IS	R-IS	K-IS	
3	0	4	5	7	-1	3	2	5	Mild K

5.4.2.4 Bi-modal classification

Bi-modal classification is defined as a person who has strong preferences in two out of four types of VARK learning styles. The result shows that none of the participants gained the highest improvement score in line with their preferred learning styles except participant 20. Referring to Table 32, participant ID 25 had a negative score for V-IS and a score of '0' for the remaining improvement scores. This person may not have focussed during the study session. Three of them were classified as V; however; their improvement scores did not demonstrate the effectiveness of the learning materials given to them.

Table 32 Detailed scores of bi-modal participants

ID	VARK Score				Improvement Score				Classification
	V	A	R	K	V-IS	A-IS	R-IS	K-IS	
6	1	6	6	4	0	1	0	3	AR
20	9	4	8	5	0	4	4	1	VR
28	7	0	8	4	0	1	2	4	VR
25	7	8	2	4	-1	0	0	0	VA

5.4.2.5 Tri-modal classification

When a person has been classified as tri-modal, this means that he/she has three preferences in terms of VARK learning style. The result in Table 33 shows that seven of the total participants were identified as tri-modal. Five of them scored highest in improvement scores which matched their learning preferences.

Chapter 5 – The Study of Improving Information Security Practices

None of them scored highest in V-IS, even though they preferred V learning style in the VARK test. This may be due to the learning material for visual, which was claimed to be difficult by some participants during the study session.

Table 33 Detailed scores of tri-modal participants

ID	VARK Score				Improvement Score				Classification
	V	A	R	K	V-IS	A-IS	R-IS	K-IS	
21	11	6	11	12	1	4	3	2	VRK
35	5	3	6	6	0	2	1	5	VRK
38	11	5	14	10	2	2	2	4	VRK
40	10	4	12	11	2	-1	3	0	VRK
17	13	13	6	12	0	-1	3	-1	VAK
31	6	6	1	5	-1	0	3	0	VAK
34	5	5	3	5	-1	3	0	3	VAK

5.4.2.6 Quad-modal classification (VARK)

Quad-modal is also known as VARK type of learning preferences (Fleming, 2006). This type of learning styles is the most popular amongst the participants. Table 34 illustrates the detailed scores of VARK learning styles:

Table 34 Detailed scores of quad-modal participants

ID	VARK Score				Improvement Score			
	V	A	R	K	V-IS	A-IS	R-IS	K-IS
1	13	9	11	9	1	3	1	1
2	4	5	3	4	-1	0	3	2
4	10	9	13	11	-1	0	1	2
5	8	9	5	6	2	2	-1	2
7	6	11	12	9	-3	0	3	4
8	7	8	7	6	2	3	-1	3
9	8	8	10	7	2	0	2	1
10	6	8	10	4	1	3	3	2
13	13	11	11	12	4	3	2	2
14	7	4	7	6	1	3	6	1
15	7	8	12	11	2	0	2	3
16	9	9	8	7	2	1	2	3
18	10	7	11	10	1	0	3	2
19	6	8	4	5	0	0	5	0
24	6	7	8	5	1	1	4	4
26	8	12	4	10	0	0	3	3
27	7	5	10	6	-1	-2	2	2
29	6	7	7	10	2	-1	3	3
32	12	10	12	14	2	1	0	1
37	3	5	8	7	0	1	1	-1

Since this involves four learning styles preferences, each section (V, A, R and K) of the positive improvement scores indicated that matched learning styles led to improvements in the post-test score. All of the participants gained positive results in their improvement scores. Even though there were negative improvement score for nine of the total 20 participants, each of them shows that they improved in their post-test in at least two of the four VARK sections.

5.4.2.7 Dyslexic participant

Whilst the study did not aim to understand the impact that personalised learning would have upon individuals with learning difficulties, one of the participants voluntarily disclosed this information at the beginning of her experiment. She claimed to be a dyslexic student.

She requested to have the learning materials (except for Topic 2 and 4) printed on yellow paper instead of reading them on a computer screen. Despite constraints of time, the researcher tried her best to accommodate the needs of the participant. The researcher changed the font format from 'Times New Roman size 12' to 'Arial size 14'. In addition to this, line spacing for the text was changed from 'multiple' to '1.5', to help the participant. These changes were made based on the guidelines for tutors taken from Sheffield Hallam University (Sheffield Hallam University, 2011). On the VARK website, there is feedback given by school teacher from Iceland regarding the usage of VARK for dyslexic students. The school has 183 dyslexic students and they are often classified as AK, or K or VAK or A (Fleming, 2011a). This feedback is similar to the study participant who was classified as A in the VARK test. She scored highest for her A-IS, V-IS and K-IS but had a negative score for R-IS (refer to Table 35). Indeed, this person indicated that she did not prefer to read, as it caused eye-strain, especially when she needed to read from a computer screen. Moreover, she stated her preferences for aural rather than read/write learning materials. This shows that using a learning styles approach for learning materials may benefits individual with learning difficulties such as dyslexia.

Chapter 5 – The Study of Improving Information Security Practices

Table 35 Detailed scores of a dyslexic participant

ID	VARK Score				Improvement Score				Classification
	V	A	R	K	V-IS	A-IS	R-IS	K-IS	
33	8	15	2	10	1	3	-2	3	Mild A

5.4.3 Further Analysis

Aside from analysing the results based on the VARK classifications, as suggested by Fleming, the experiment results were analysed by comparing the Improvement score and the VARK score for each participant. The analyses were made by grouping the participants into these categories, as listed below:

a) Highest VARK score and Highest Improvement Score (HH):

- Highest Visual in the VARK score and Highest Visual in the Improvement Score;
- Highest Aural in the VARK score and Highest Aural in the Improvement Score;
- Highest Read/write in the VARK score and Highest Read/write in the Improvement Score;
- Highest Kinaesthetic in the VARK score and Highest Kinaesthetic in the Improvement Score.

b) Second highest VARK score and Highest Improvement Score (2HH):

- Second highest Visual in the VARK score and Highest Visual in the Improvement Score;
- Second highest Aural in the VARK score and Highest Aural in the Improvement Score;
- Second highest Read/write in the VARK score and Highest Read/write in the Improvement Score;
- Second highest Kinaesthetic in the VARK score and Highest Kinaesthetic in the Improvement Score.

Chapter 5 – The Study of Improving Information Security Practices

- c) Lowest VARK score and Lowest Improvement score:
- Lowest Visual in the VARK score and Lowest Visual in the Improvement Score;
 - Lowest Aural in the VARK score and Lowest Aural in the Improvement Score;
 - Lowest Read/write in the VARK score and Lowest Read/write in the Improvement Score;
 - Lowest Kinaesthetic in the VARK score and Lowest Kinaesthetic in the Improvement Score.
- d) Other – Participants that do not fall into any of the above categories: for example, those who scored highest Visual in VARK score and score highest Aural in the Improvement Score.

Those results with HH, 2HH and LL categories are considered to be positive results. This is because the researcher assumes that those who score highly in the VARK test will obtain high improvement scores. In other words, those who score high in VARK should perform well in the post-test after go through the learning materials that suit their learning preferences. For example, a participant who scores highly in the Visual in VARK test should have a high score for his improvement score in the visual section. As referred to in Table 36 below, 80% of the total participants' results are positive. For the 2HH results, the average differences of score between the highest and the second highest of VARK score was 2.8. Since there is only a small difference of score between the two categories, the 2HH category may be considered to show positive results in this case. The average differences of the VARK score between the highest and the third highest was 4.1. Therefore, the researcher decided not to consider the third highest score as the positive results Other positive results are those with LL category.

Chapter 5 – The Study of Improving Information Security Practices

This is because those who score lowest in the VARK test should score low in their Improvement scores. The result demonstrates the validity of the VARK test, and also tells us that learning materials tailored into individual preferences do help the learning process for at least 80% of the participants in the study

The summaries of the findings are presented in Table 36.

Table 36 Analysis of the participants' VARK and the Improvement Scores

Remarks	No of Participants	Learning Styles Mode and no. of participants
Highest VARK Score and Highest Improvement Score (HH)	7	A=1 VAK=1 VRK=1 VARK=4
2 nd Highest VARK Score and Highest Improvement Score (2HH)	7	MILD R=1 VR=1 AR=1 VARK =4
Lowest VARK Score and Lowest Improvement Score (LL)	3	VRK=1 VARK=2
HH and 2HH	3	VARK=3
HH and LL	6	MILD K=1 STRONG A=1 VRK=1 VARK=3
HH, 2HH and LL	2	MILD A=1 VARK=1
2HH and LL	4	MILD A=1 MILD R=2 STRONG R=1.
Other	8	VA=1 VR=1 VAK=2 VRK=1 VARK=3
Total	40	

For further detailed analysis of the data, Table 37 was extracted from the results. The majority of HH were classified as quad-modal VARK, followed by tri-modal and uni-modal. Referring to Table 37 below, the last column shows the learning styles ranked by participants. Participants were asked to rank the four modalities according to the most preferred to the least preferred.

Chapter 5 – The Study of Improving Information Security Practices

The initial letters of the four learning styles were arranged according to the rating made by the participants. For example, participant ID 8 has ranked KVRA where Kinaesthetic is the most preferred, followed by Visual, Read/write and Aural as the least preferred mode. Overall, almost all participants scored highest in the VARK test and ranked a particular mode as the most preferred styles. For example, participant ID 22 ranked Aural as the most preferred and scored the highest in Aural (A) VARK test and Improvement Score (A-IS). This result implies that what participant think of their preferred learning styles is matched with their VARK test results. In addition to this, they scored well in the post test for that particular learning style. Therefore, this demonstrates that learning preferences does contribute to better learning where information security topics are concerned.

Table 37 Detailed scores for participants who scored the highest VARK and highest improvement scores

No	Participant ID	VARK Scores				Improvement Scores				Classification	Rank VARK
		V	A	R	K	V-IS	A-IS	R-IS	K-IS		
1	8	7	8	7	6	2	3	-1	3	VARK	KVRA
2	14	7	4	7	6	1	3	6	1	VARK	KARV
3	22	0	9	5	2	0	2	-2	0	A	AKRV
4	24	6	7	8	5	1	1	4	4	VARK	KRAV
5	34	5	5	3	5	-1	3	0	3	VAK	VKAR
6	35	5	3	6	6	0	2	1	5	VRK	KRAV
7	37	3	5	8	7	0	1	1	1	VARK	RKAV
TOTAL		0	3	3	2		3	3	2		

Amongst the HH category, 3 out of 7 participants (refer to Table 37) scored highest in the Aural (VARK test) and improvement score. The same amount of participants (3) scored highest in Read/Write (VARK test) and improvement scores. Only two of the total participants in the HH category scored highest in Kinaesthetic (VARK and Improvement score). However, none of the participants scored highest in Visual for the category. The result illustrates that people with matched learning styles A, R and K performed well in the post-test. Nonetheless, learning materials for visual were not helpful to this category.

Chapter 5 – The Study of Improving Information Security Practices

In terms of ranked VARK from the participants obtained in Part 4, the users' experience survey, only three of the total seven participants had their choice matched with the highest VARK result. This however, happens sometimes where participants think that they prefer a certain learning style, but in fact, they prefer other learning styles. Hence, learning style test is required to help people to know their learning preferences in order to maximise their learning capabilities.

Again, Table 38 was derived from the whole results from further analysis on the 2HH respondents. The majority of them were quad-modal VARK, followed by bi-modal and uni-modal. It appears that kinaesthetic learning materials do have a good impact on the participants during the study session. Five of the total seven participants in the category scored highest in Kinaesthetic, one of them was in Visual and another in Read/Write learning styles. In this category, nobody scored high in Aural. As regards rank VARK, five of the total participants in the category score highest in the learning styles that they most preferred. The same indication may assume that learning style improves learners' performance when it matches their learning preferences.

Table 38 Detailed scores for participants who scored the second highest VARK and highest improvement scores

No	Participant ID	VARK Scores				Improvement Scores				Classification	Rank VARK
		V	A	R	K	V-IS	A-IS	R-IS	K-IS		
1	4	10	9	13	11	-1	0	1	2	VARK	KARV
2	6	1	6	6	4	0	1	0	3	AR	KARV
3	12	3	4	8	5	0	-1	1	4	Mild R	AKRV
4	15	7	8	12	11	2	0	2	3	VARK	KVRA
5	20	9	4	8	5	0	4	4	1	VR	RKAV
6	26	8	12	4	10	0	0	3	3	VARK	KAVR
7	32	12	10	12	14	2	1	0	1	VARK	KARV
TOTAL		1	0	1	5	1	0	1	5		

For LL participants, only three of the total respondents as can be seen in Table 39 below. This result also indicates that the least preferred learning styles resulted in the lowest improvement score.

Chapter 5 – The Study of Improving Information Security Practices

It is logical that if a person does not like a certain learning style, the person has the tendency to perform less well using this style than their preferred learning styles.

Table 39 Detailed score for participants scored lowest VARK and lowest improvement scores

No	Participant ID	VARK Score				Improvement Score				Classification	Rank VARK
		V	A	R	K	V-IS	A-IS	R-IS	K-IS		
1	1	13	9	11	9	1	3	1	1	VARK	RVKA
2	7	6	11	12	9	-3	0	3	4	VARK	AVKR
3	38	11	5	14	10	2	2	2	4	VRK	RVKA
TOTAL		1	1	0	1	1	1	0	1		

Referring to Table 40, 9 of the total participants' scores showed positive improvements. Positive improvement scores indicated that there are improvements in the post-test score as compared to pre-test. These improvements suggest that learning styles do provide a positive impact on learning security topics. It may also be assumed that the learning materials are able to disseminate new information to participants.

Table 40 Detailed score for participants who has only positive improvement scores

No	Participant ID	VARK Score				Improvement Score				Classification	Rank VARK
		V	A	R	K	V-IS	A-IS	R-IS	K-IS		
1	1	13	9	11	9	1	3	1	1	VARK	RVKA
2	10	6	8	10	4	1	3	3	2	VARK	RKAV
3	11	2	8	2	4	1	3	1	2	STRONG A	RVAK
4	13	13	11	11	12	4	3	2	2	VARK	AKVR
5	14	7	4	7	6	1	3	6	1	VARK	KARV
6	16	9	9	8	7	2	1	2	3	VARK	KVAR
7	21	11	6	11	12	1	4	3	2	VRK	VARK
8	24	6	7	8	5	1	1	4	4	VARK	KRAV
9	38	11	5	14	10	2	2	2	4	VRK	RVKA

Previous discussions have concerned matching learning preferences with performance. The next discussion now focuses on mismatched learning preferences, which may be defined as follows:

- a) Participants with the highest VARK score and with a negative improvement score
- b) Participants with second highest VARK score and with a negative improvement score

Chapter 5 – The Study of Improving Information Security Practices

A total of 25% of the participants were identified as having mismatched learning styles. Five of them were considered as mismatched for visual, three for aural, two for read/write and kinaesthetic respectively.(refer to Table 41) The possible reason why people did not score in the visual learning materials section is the learning materials is difficult in nature. In addition to this, participants gave poor ratings for learning materials created for visual learners.

Table 41 Detailed scores of participants with mismatched learning style

No	Participant ID	VARK Score				Improvement Score				Classification
		V	A	R	K	V-IS	A-IS	R-IS	K-IS	
1	2	4	5	3	4	-1	0	3	2	VARK
2	8	7	8	7	6	2	3	-1	3	VARK
3	17	13	13	6	12	0	-1	3	-1	VAK
4	22	0	9	5	2	0	2	-2	0	A
5	25	7	8	2	4	-1	0	0	0	VA
6	27	7	5	10	6	-1	-2	2	2	VARK
7	29	6	7	7	10	2	-1	3	3	VARK
8	31	6	6	1	5	-1	0	3	0	VAK
9	34	5	5	3	5	-1	3	0	3	VAK
10	37	3	5	8	7	0	1	1	-1	VARK

5.5 Discussion

The results demonstrate that the majority of the male participants prefer the four ways of learning, as compared to their female counterparts. Most of the participants at least hold a Bachelor's degree or above, since in most cases they are. This is because most of them are students and staff of Plymouth University. A total of 24% of the participants are uni-modal; 11% are bi-modal and 16% have tri-modal learning styles. These show that there is a need for tailoring learning materials based on their preferences. Moreover, 80% of the total participants show that learning styles have a positive effect on their learning process.

The results were analysed in two ways; first, they were based on the VARK classification, where the participants were grouped based on their VARK result (refer to the sub-section 5.4.2 Analysis based on VARK classification) such as uni-modal, bi-modal, tri-modal, and quad-modal learning styles.

Second, the result were analysed based on the classification that the researcher made (refer to sub-section 5.4.3 Further Analysis). Both the sets of results showed positive results. For the VARK classification analysis, three out of the four uni-modal Aural scored highest in Aural improvement scores, five out of seven tri-modal scored the highest in their matched learning styles, and all of the quad-modal participants showed improvements in their post-test section that matched their learning styles. For the second analysis, the results were promising, with 80% of participants having achieved positive results.

5.6 Conclusion

In summary, the majority of the participants are multimodal rather than having single learning preferences. Multimodal people are more flexible in learning, as long as they feel comfortable in using all types of learning styles. In conclusion, learning styles do give good insights toward learning process within the information security area.

6 The Personalising Information Security Education (PISE) Framework

6.1 Introduction

Having identified that a personalised learning approach has a positive role to play in improving information security awareness, the next phase of the research focuses upon how to develop a framework that will enable a personalised learning system for people to be realised at a practical level.

Personalised learning is also referred to as individualised learning in schools (Sebba *et al.*, 2007); however, as Johnson (2004a) has suggested, using the 'individualised learning' term is a bit unrealistic due to the fact that it giving more pressure to the creator of the learning materials to create the exact materials for each individual person. By contrast, 'personalised learning' can refer to a whole class, a small group or a one-to-one basis of people with the same preferences in learning (Sebba *et al.*, 2007). Therefore, the framework has been named as personalised, rather than individualised information security education. The Personalising Information Security Education (PISE) needs to be a flexible, user friendly and accessible in the user's own time. The framework seeks to help the user to learn information security and improve security practices. However, there are a number of requirements that need to be carefully defined, in order for such a system to be operational and acceptable. This chapter introduces these requirements and the framework that has been designed to capitalise upon the unique features in aiding the learning process.

6.2 System Requirements

The framework is proposed with an element of learning styles to help people in learning information security in their organisation.

A practical implementation (PISE) was designed based on the framework proposed. PISE consists of two types of systems; Private PISE, which is a private system for an organisation, and Public PISE whereby everyone can access to the system. The latter has been proposed to account for the home user aspect. Both systems are web-based systems, by which organisations and the public may be able to access the system via the Internet or Intranet.

6.3 PISE Model

PISE model comprises the five components below:

- 1) Users :
 - a. Private trainee – an employee in an organisation who uses Private PISE system.
 - b. Public trainee – a person who uses Public PISE system.
 - c. PISE system administrator (PSA) – a person who controls the whole systems, including Private and Public PISE systems.
 - d. Private PISE Training Course Administrator – an organisations' employee who is responsible for managing modules and assessment packages for employees in the organisation (Private trainee).
 - e. Public PISE Training Course Administrator – an individual who is responsible for managing modules and assessment packages for Public trainee.

- 2) Learning styles test – stakeholders could choose which learning styles they would like to use for their PISE system. For illustration purposes, the researcher use VARK test as an example.

- 3) Learning materials database includes:
 - a. Organisations' Syllabus – syllabus that is tailored-made for the particular organisation or company information security policy.

- b. Learning materials from the external organisation that specialised in information security (for example, European Network and Information Security Agency (ENISA), British Computer Society (BCS), National Institute of Standards and Technology (NIST) and International Information Systems Security Certification Consortium Incorporation (ISC)²)
 - c. Other learning materials uploaded by public trainees.
- 4) Assessments database – the database is meant to store all the quizzes for the pre and post-assessments
 - 5) User profile database – a database to store trainees' information (e.g. personal details, educational background, learning styles results, personalised learning plans, assessment results) and also administrators information.

The framework is developed based on the Analysis, Design, Development, Implementation and Evaluation (ADDIE) model, and comprises five basic steps (Kovalchick and Dawson, 2003). The model originates from the instructional systems development (ISD) model (Husen and Postlethwaite, 1994). The ADDIE processes are illustrated in Figure 34 below. ADDIE is a common and effective model used by instructional designers and training developers (Molenda, 2003). The processes are recursive, and will be continuous as long as there are updates and development of the learning materials. The five basic steps of the model are as follows:

- 1) Analysis – defined as a step to identify what to be learnt and by analysing the previous knowledge and skills.
- 2) Design – the phase deals with designing learning objectives on how to the individual should learn.
- 3) Development – is a process where the learning materials, pre and post-assessments are created to suite with the learners' existing knowledge

- 4) Implementation – a phase where learners start to do pre and post-assessments and personalised learning provided by the developers.
- 5) Evaluation – the step is to ensure the materials are up to date, and all other processes are effective.

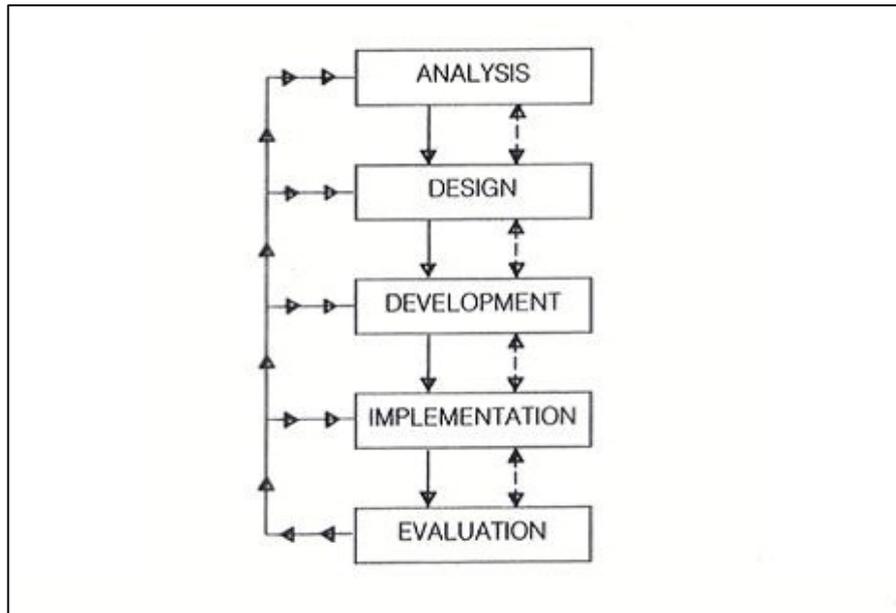


Figure 34 ADDIE processes

*Source: (Molenda, 2003)

Figure 35 and Figure 36 below show the proposed framework for the improvement of the information security learning process. The framework has five phases, and this is adopted from the ADDIE processes. The framework proposed only implements the first two phases, which are analysis and design. This is because the limitation of time available for the researcher to develop the materials, implement and evaluate the complete system. However, the study conducted on the effectiveness of learning styles upon learning information security topic showed the effectiveness of the approach, similar to the framework proposed.

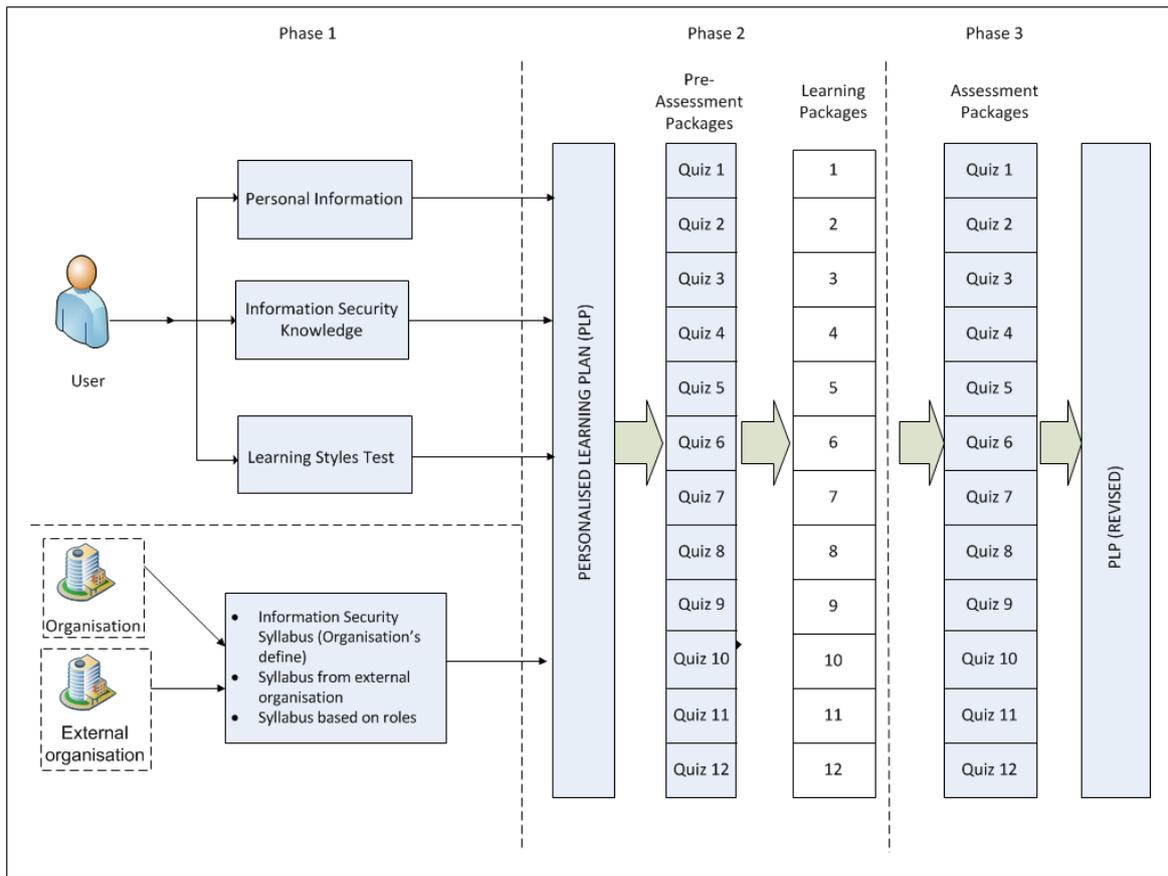


Figure 35 Proposed PISE framework

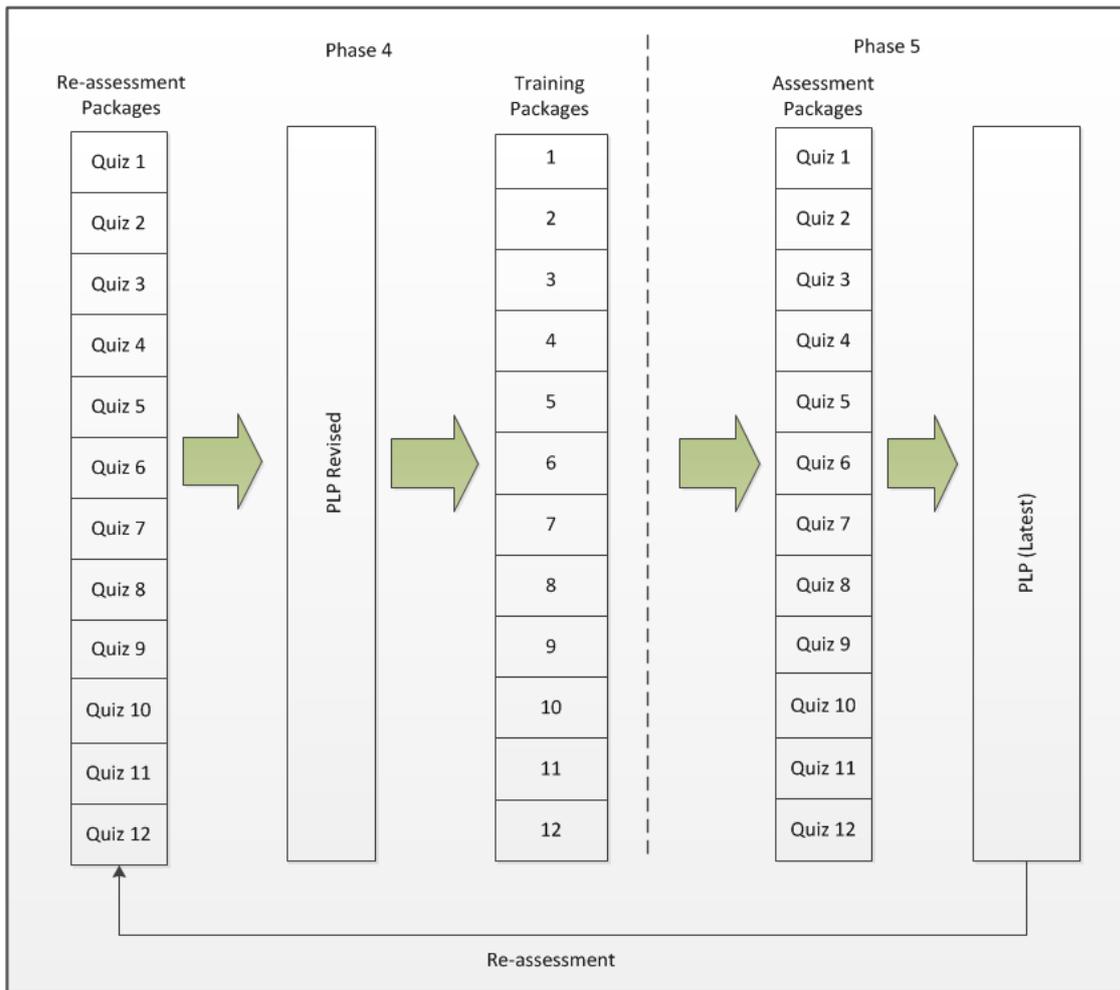


Figure 36 Proposed PISE framework continue

Phase one is the collection of information on the user and organisation, which is similar to the analysis process in ADDIE. The user will give personal information (name, educational background), and information on security knowledge (attended digital forensic course, involve in the information security campaign or attended biometric seminar). The user then takes a learning style test, in this case a VARK test, available online. The organisation course administrator will then upload the company’s information security syllabus tailored to the organisation, or they can adopt other syllabus from the external organisations (such as ENISA/NIST/(ISC)²) mentioned in the previous sub-section. The framework provides flexibility in terms of choosing a syllabus that best suits the company.

Phase two (see Figure 35) consists of a personalised learning plan generated by the system based upon information given by the user. Referred to as the ADDIE model, this phase is still under the analysis process, whereby the information on users' pre-knowledge is yet to be obtained. The user then needs to take pre-assessment packages, which include all topics (pre-selected by organisation's training course administrator based on users' role), in the syllabus (for the first time user only), in order to measure which topic the users are familiar with and need to undergo training. This means that all topics for office administrators' role will be different from those for network administrators. The pre-assessment will save users' time, as they can be exempted from the topic that they do not need to know, based on their roles in the workplace, topics that they are familiar with, or have attended related trainings for information security, before they use the system. The reason why users need to be assessed against all the topics is to assess their pre-existed knowledge gained not only from formal training, but also from informal discussions with friends or experiences. This mechanism also helps to determine whether what users claimed to know is true, or they just make it up. After they have obtained the pre-assessment results, users will be able to view their personalised learning plan, which consists of the training packages that they need to complete. This is where the design and development phase of ADDIE model is adopted. In this phase, the users will be able to select training packages that suit their preferred learning styles.

Next, users should be able to access to the training via online in their own time. However, the user needs to complete certain training packages with a specific time frame (for example, user need to complete training pack that is classified as very important for their roles in an organisation prior to the one that is more general in nature) as defined by the organisation's training course administrator. This stage is where the implementation of the learning materials is applied, as specified in the ADDIE model. This is also where the

personalised learning objectives are met and will help users in their learning process (Dainton, 2004).

Moving on to phase three, which consists of assessment packages and revised PLP, after users have completed training packages, they will take quizzes to evaluate their knowledge obtained from the training. If the user passes, then their PLP will be updated, and they will be notified by the organisation's training course administrator for the next training packages to be completed. In case the user does not pass the evaluation, they will need to repeat the training package and the assessment until they pass. Once they have finished the assessment, the system will generate a revised PLP which includes updated training package the user has completed recently.

After three to six months, depending on the organisation's policy, user will be entering phase four (see Figure 36) where they will need to be re-assess in order to refresh their memory and to update their current security knowledge. The time interval is suggested because the effect of the training attended could be determined after at least three to six months (Mohd Noor and Dola, 2012). It is a recurrent process, and similar to phase two and three. At the end of phase four, the user will undergo required training packages based on the assessment results and proceed to the next phase.

Phase five is the final phase. However, it is a cycle where after a certain time; users need to be re-assessed in order to maintain awareness of security and practices. Based on the framework, two types of systems; Private and Public PISE are proposed.

6.4 PISE Implementation

The PISE system is proposed to be a web based system, because it is a flexible education platform and it is widely accepted that learning could take place anywhere and anytime through any computer (Liu and Chen, 2008; Syed-Khuzzan and Goulding, 2009). The possible software and hardware needed for the system are a database (e.g. MySQL), programming languages to code the system interface (e.g. Visual Basic), server (e.g. Windows Server) and printer for report generation. It is proposed that the system will be web-based, and that the user will be able to access it from anywhere, provided they have an Internet connection. Below are the requirements for users to use the system:

- a) personal computer (PC)/iPad/Tablet PC;
- b) Internet connection;
- c) Internet browser;
- d) printer and paper (optional);
- e) username and password to login into the system.

The PISE is a centralised repository maintained by the PISE system administrator. Since the system consists of two types of systems, the private and public PISE have their own administrators, as will be discussed in the next two sub-sections.

6.4.1 Private PISE

The Private PISE model is proposed for the use of the organisation, for its employees. Each user will register to the Private PISE system prior to the role's input by the training administrator. Each organisation will have its own Private PISE Training administrator to manage the trainee in the organisation. Users will be able to view their profile, containing personal information and other information regarding their training.

For further information on how the Private PISE would work, system flowcharts are used to represent the system flow based on the user's role. System flowcharts explain the flow of data throughout a system (IBM Corporation, 1970; Jacobson *et al.*, 1992; Martin, 2009) in a graphical representation. In the thesis, the International Business Machines (IBM)-flowcharting techniques-GC20-8152-I which includes the standard flowchart symbols that follows the American National Standards (ANS); ANS Standards X3.5-1970 Flowchart Standard is adopted in order to have a clear and understandable diagrams (IBM Corporation, 1970; Chapin, 1979). The basic symbol is shown in the Figure 37 below:

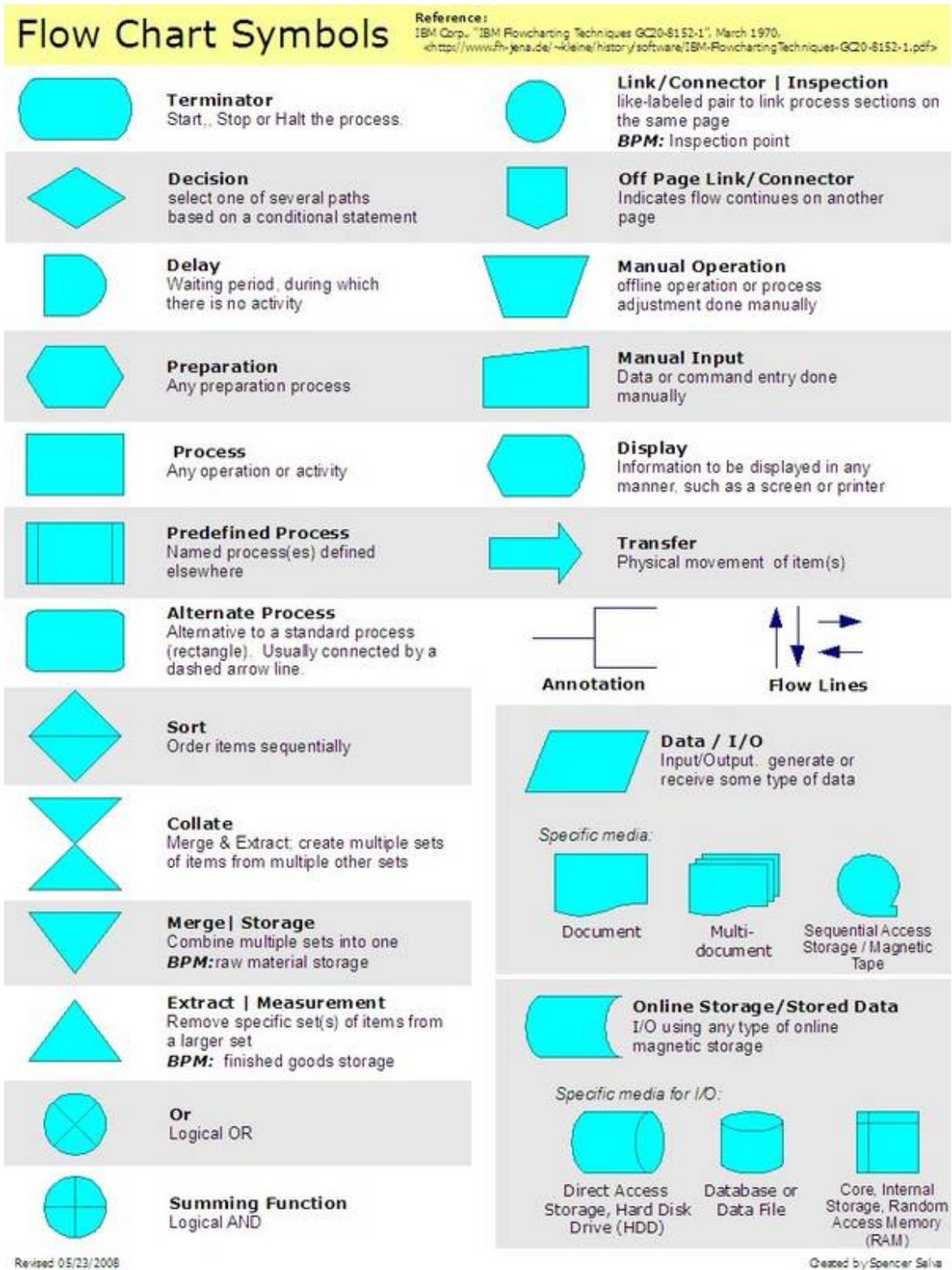


Figure 37 Flowchart symbols

*Source: (Neha, 2013)

There are three categories of main users in the system; Private trainee, PISE system administrator, and Private PISE training course administrator. The roles for each entity are summarised in Table 42:

Table 42 Summary of users' roles for Private PISE System

Title	Roles
Private trainee	The user for the Private PISE system. Some might have a specific role such as Private PISE Training Course Administrator.
PISE System Administrator	Responsible for maintenance of other users in the PISE system (including both Private and Public PISE system). Provide administrative support to all PISE users.
Private PISE Training Course Administrator	The person is responsible for managing Private trainees in an organisation. The person updates, and maintain trainee's information for the system. The person also responsible to manage and maintain modules and assessments within the Private PISE system. Provides administrative supports to all Private PISE users.

The system flowcharts are organised based on each user of the system. For example, the first user flowchart (see Figure 38 and Figure 39) will demonstrate the system flow for Private trainee, followed by PISE System Administrator (see Figure 40 and Figure 41) and Private PISE Training Course Administrator (see Figure 42). Figure 38 shows private trainee needs to know their learning styles and get approval from the PISE System Administrator before register to the system. If the trainee does not know his/her learning styles, they need to take the VARK test via VARK website and key in the result before submit the registration form to the system. The approval is needed to ensure the trainee has keyed-in the correct

information related to his/her organisation where he works. Later, the trainee will have to sit for the pre-test in order to know his current knowledge on information security. After viewing the result of the pre-test, then the trainee can start select the learning modules and use the other services provided by PISE system.

Figure 39 represents the processes for the private trainee in the PISE system after they completed the registration processes. The trainee could choose to learn the modules (Do learning) where he/she can select the modules based on learning styles results. After learning the modules he/she can decide to proceed with the assessment (Do assessment) for the particular module or to exit the session and do the assessment later. The trainee also could choose to do view results for the assessments and edit their personal details (Edit profile) in the system.

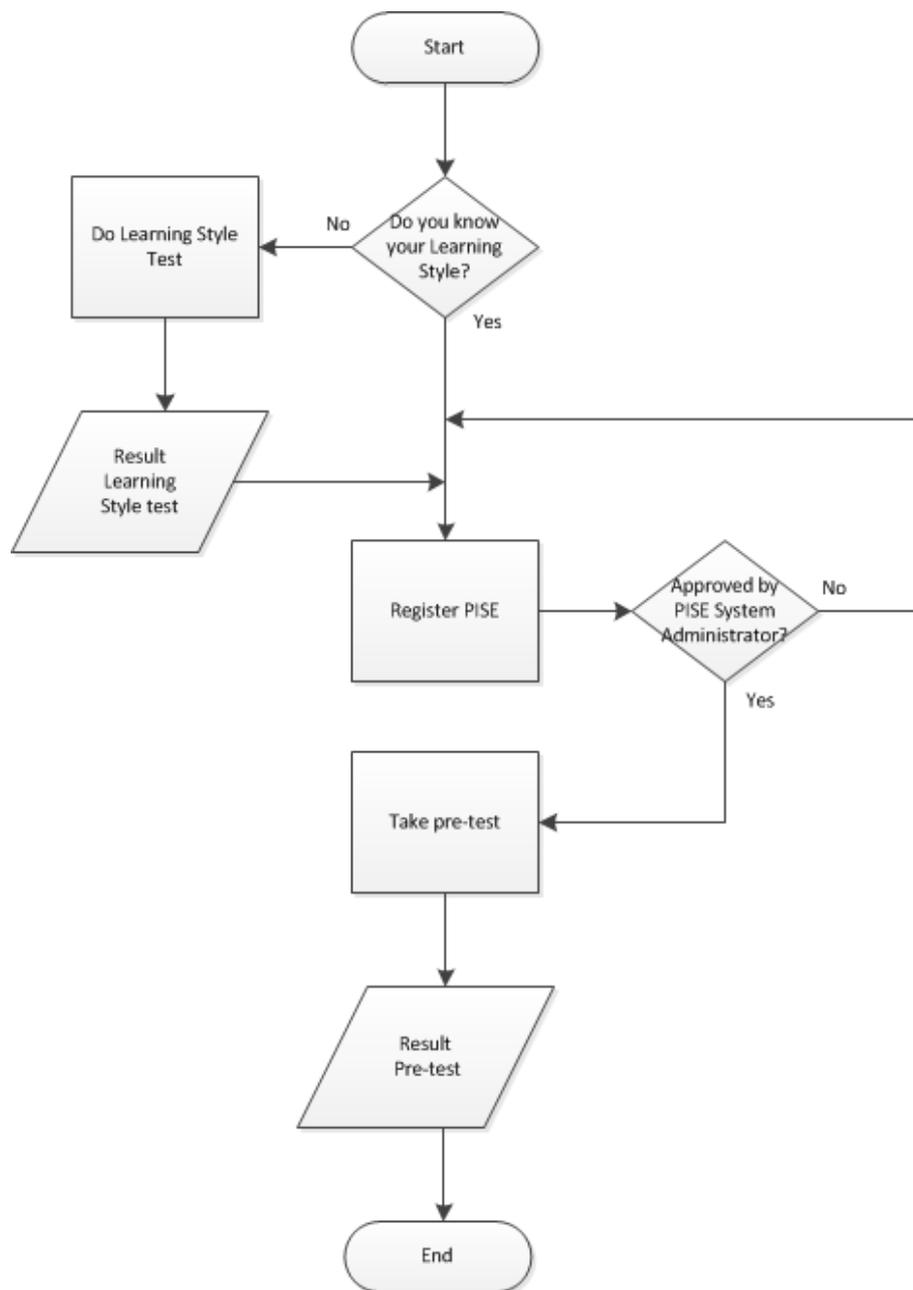


Figure 38 The Registration flowcharts for Private Trainee

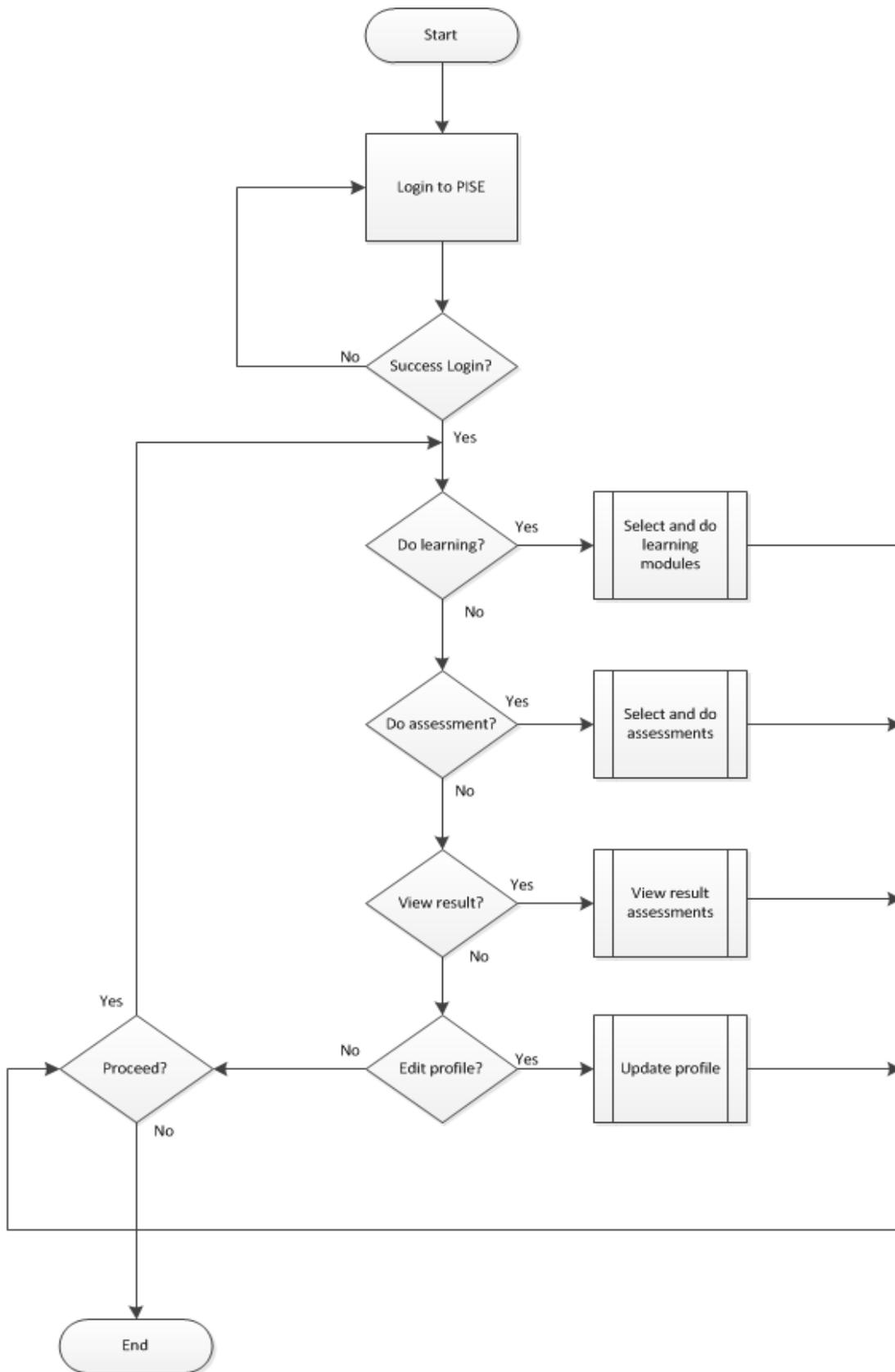


Figure 39 Flowcharts for Private trainee

Figure 40 below presents the process flow for the PISE System Administrator. After login, the system administrator is able to choose to enter the Private PISE system or Public PISE system. Each of the sub-processes denoted by “Enter Private PISE” and “Enter Public PISE” has its own process flow. When the system administrator enters the Private PISE system, the processes are shown in the next flowchart (see Figure 41). In Figure 41, the system admin could choose to verify and edit trainee or manage modules. See diamond shapes “Verify Trainee”, “Edit Trainee” and “Manage Module”. The system administrator could choose to proceed to other tasks or to exit the system. The “Approve/reject trainee” is a process where the admin verify the information in the Private trainees’ registration forms. For example, if the trainee mistakenly keyed-in the wrong position in their organisation, the PISE System Administrator can reject the application and the trainee needs to re-apply. The “Edit Private trainee” enables the admin to update the Private trainee information. The admin also could edit and manage the modules and assessments in the system.

The Private PISE Training Course Administrator provides supports to private trainee by managing modules and assessments for an organisation. The process flow for the Private Training Course Administrator is illustrated in Figure 42. The flowchart (see Figure 42) has the similar choices as the Private Trainee processes (see Figure 39). This is because; the Private Training Course Administrator is also a Private Trainee in the PISE system. The differences are; the training course admin would be able to manage modules, assessment and results for other Private Trainee.

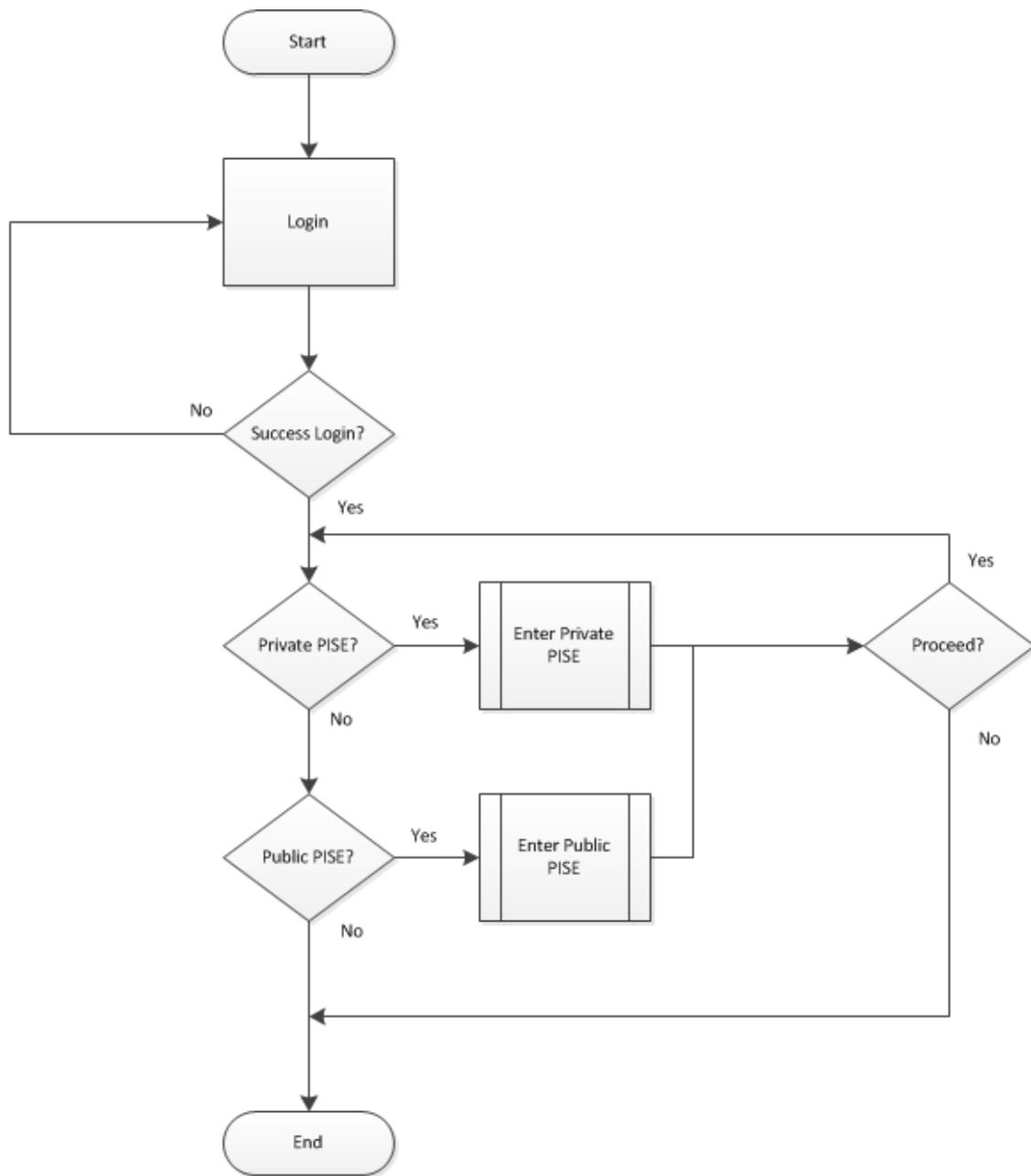


Figure 40 Flowcharts for PISE System Administrator

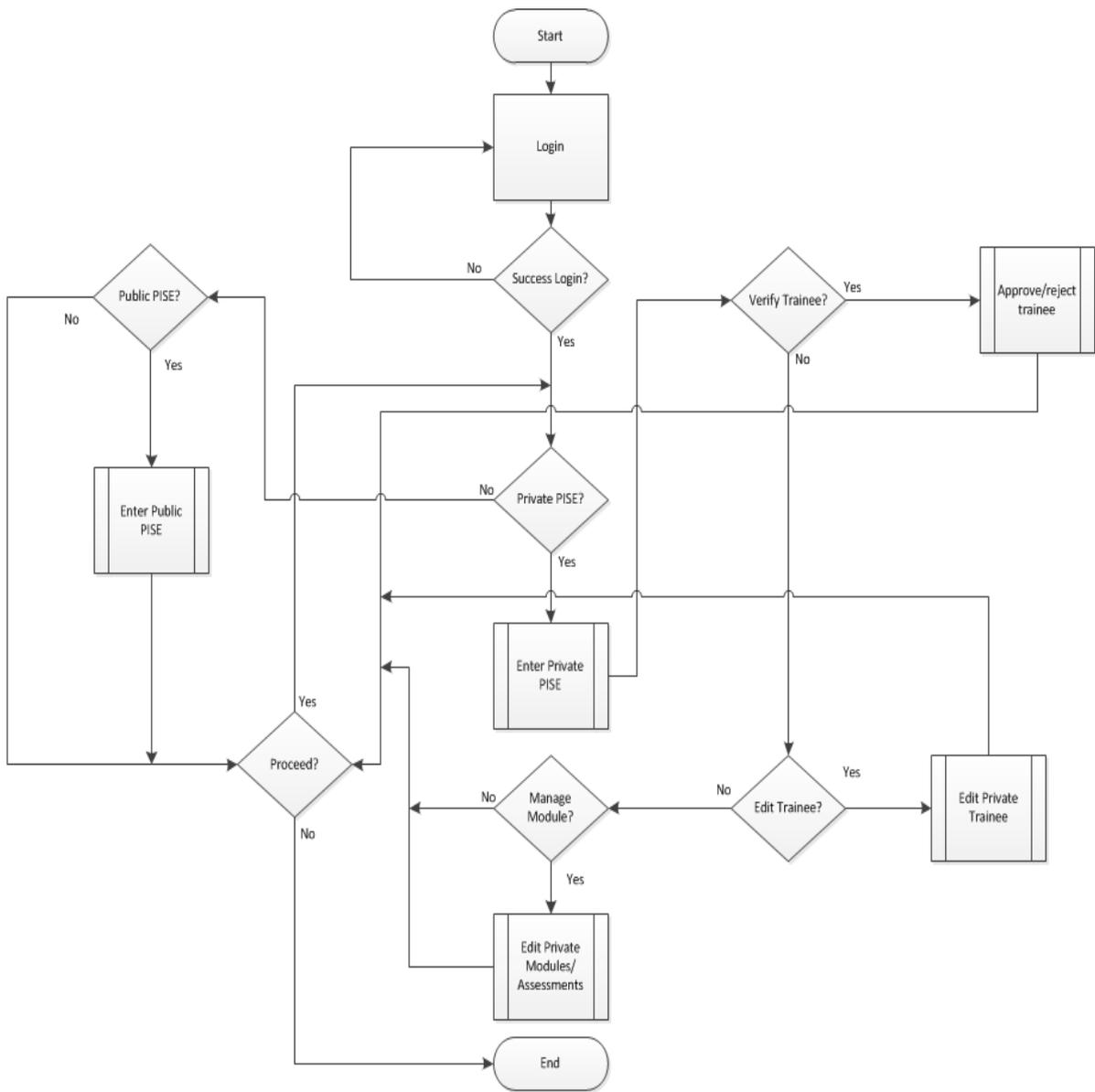


Figure 41 Flowcharts for PISE System Administrator (Private PISE)

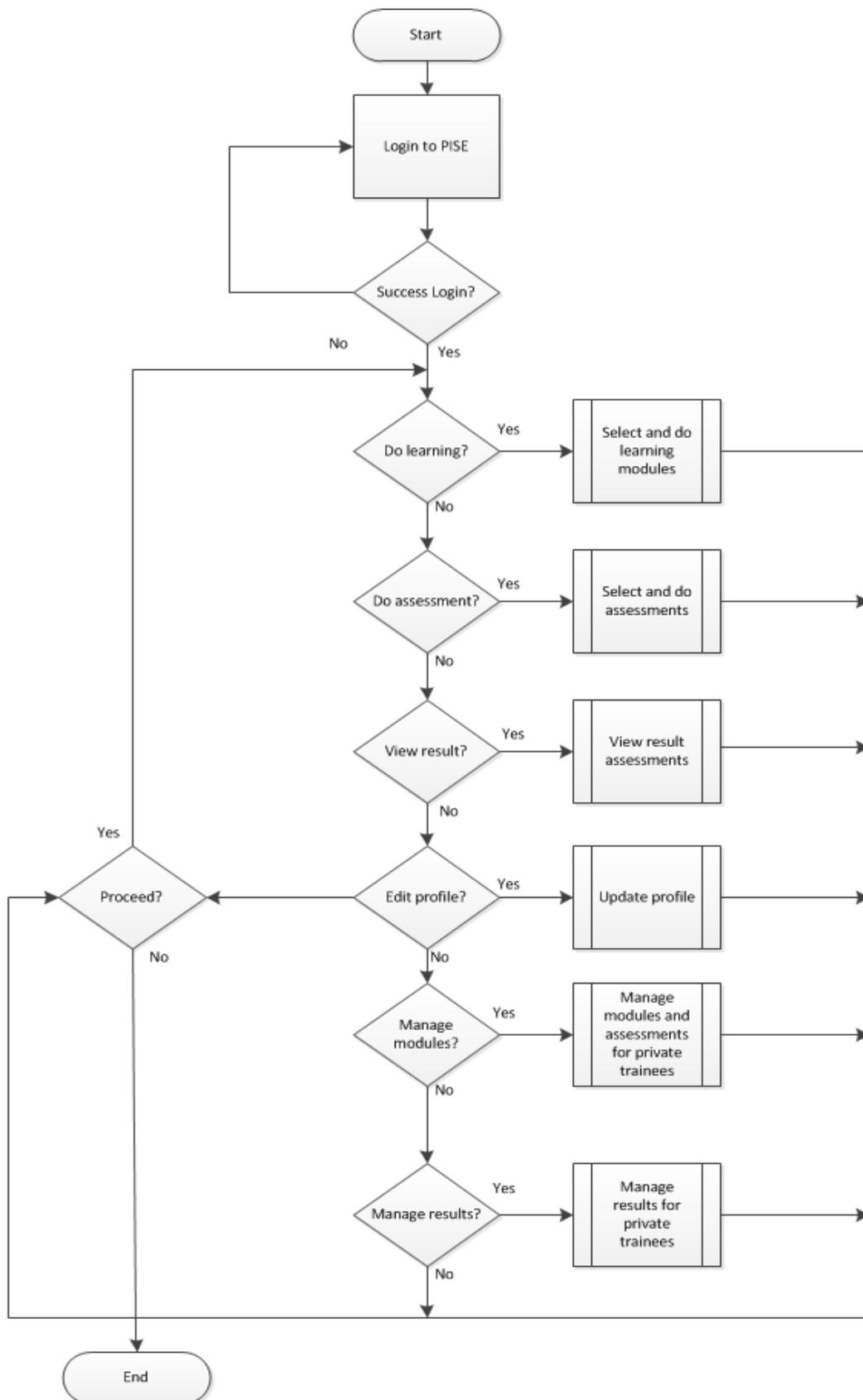


Figure 42 Flowcharts for Private PISE Training Course Administrator

6.4.2 Public PISE

Public PISE is proposed to help public users to learn and contribute to the system. The public can contribute in the sense that they might upload learning materials tailored to individual's learning styles to the system, at no cost. The model is also proposed as one of the solutions for the users' issues on sources of information security knowledge home users. Home users have problems choosing which information and from whom they should take the information. Given this, the PISE system provides a platform for the public to learn materials from the external organisations that specialised in the area (e.g. ENISA/NIST) and also from other public trainees who are experts in the information security area. The quality of the materials uploaded by public trainee will be monitored by the Public PISE Training Course Administrator. The possible method of checking the credibility of the materials is by checking the individual's professional background, so that other users can review the usefulness of the material via voting systems.

Public PISE system has three types of main users; Public Trainee, PISE System Administrator and Public PISE Training Course Administrator. The roles of the users are listed in the Table 43 below:

Table 43 Summary of users' roles for Public PISE System

Title	Roles
Public trainee	The user for the public PISE system. The trainee could upload modules and assessments to the Public PISE system. Some might have a specific role such as Public PISE Training Course Administrator.
PISE System Administrator	Responsible for maintenance of other users in the PISE system (including both Private and Public PISE system). Provide administrative support to all PISE users.
Public PISE Training Course Administrator	The person is responsible for managing Public trainees in the PISE system. The person updates, and maintains trainee's information for the system. The person also responsible to manage modules and assessments within the Public PISE system. These also include approving modules and assessments uploaded by Public trainees. The job scope involves administrative supports to all Public PISE users.

For further details on each type of user, a series of flowcharts for Public PISE system are presented in the next figures (see Figure 43 to Figure 46). Registration processes for Public trainee (see Figure 43) is similar to the Private trainee (see Figure 38) except the public trainee does not require an approval from PISE System Administrator. The flow in Figure 43 shows the processes where the trainee can take pre-test upon completing registration. The registration process completed after the trainee view the pre-test result and they can login into the Public PISE system.

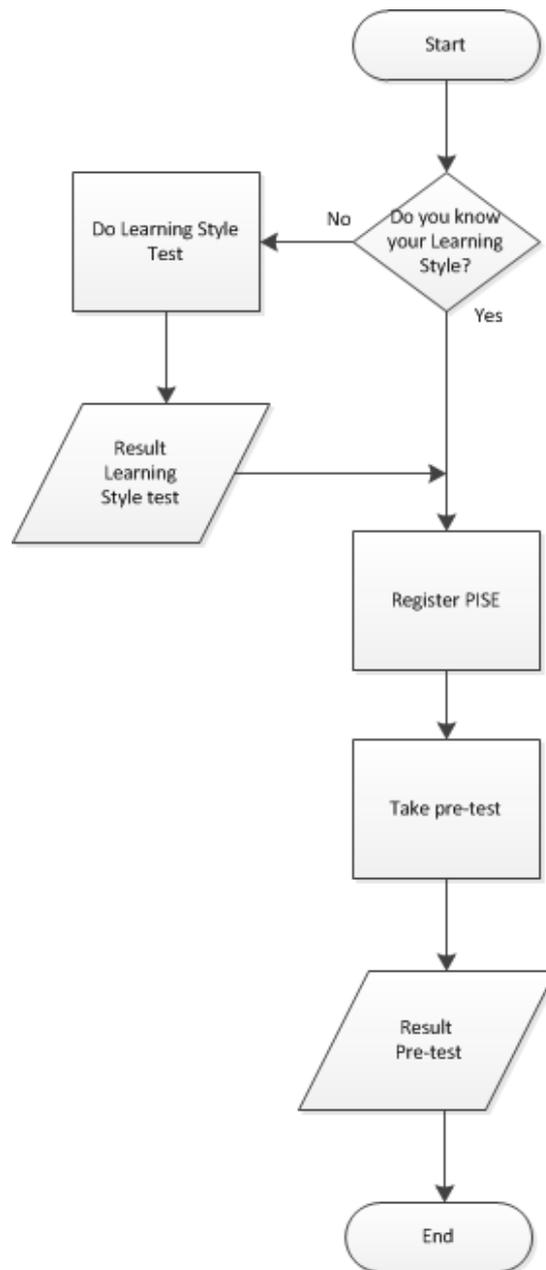


Figure 43 Flowcharts for Registration Public PISE Trainee

After complete the registration, the Public trainee can return to the system via login and

starts using the system. See Figure 44. The Public trainee has similar processes as Private trainee (see Figure 39) with additional processes “Upload learning modules and assessments”. In this process, the public trainee can upload and share learning modules together with assessment to the PISE system. These uploaded materials will need to be approved by the Public PISE Training Course Administrator before it is use in the Public System. If the trainee has new information to be updated such as the latest seminars attended, they could edit their profile in “Update profile” process. After that, the trainee can choose to proceed with other processes or to exit the session.

Figure 45 demonstrates the flow processes for PISE system administrator when dealing with Public PISE. The flow starts after the successful login and entering the Public PISE system (See process label “Enter Public PISE”). The admin can choose processes “Edit trainee” or “Manage modules”. In the “Edit Public Trainee” process, the admin could change details for the trainee such as adding role as the Public PISE system administrator. The admin also have privilege to add or edit modules and assessments.

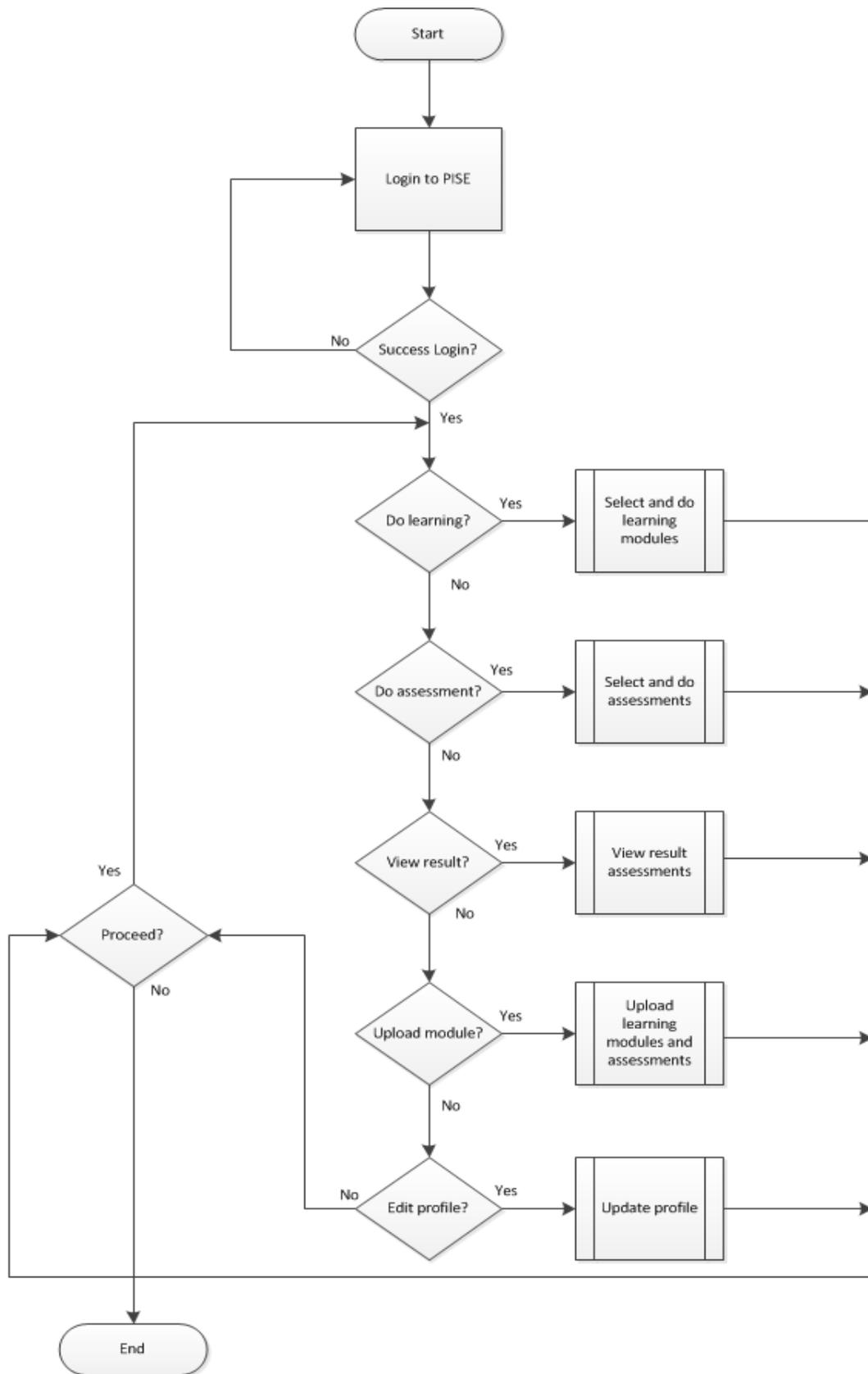


Figure 44 Flowcharts for Public Trainee

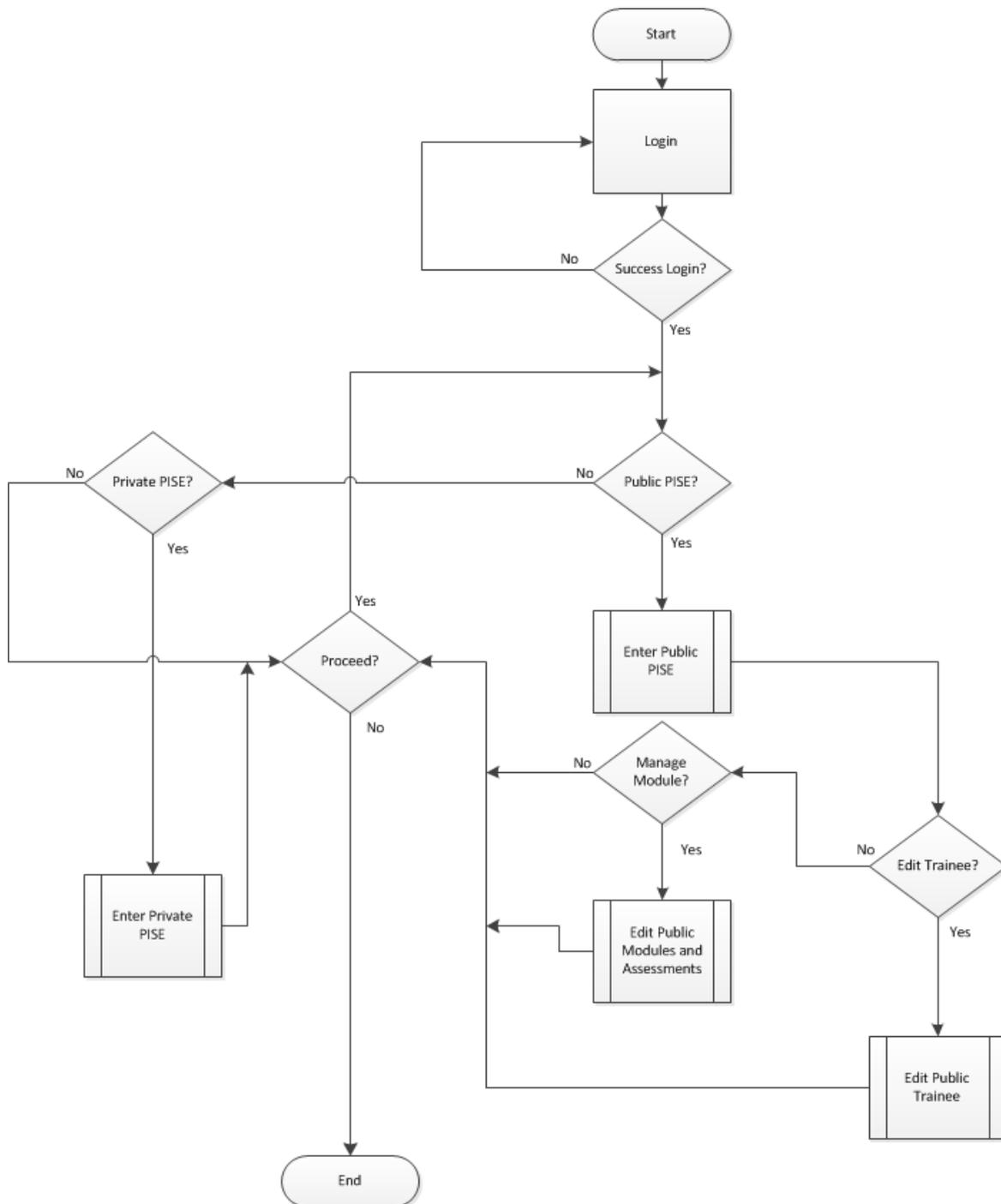


Figure 45 Flowcharts for PISE System Administrator (Public PISE)

Figure 46 represent the process flows for the Public PISE Training Course Administrator. The flow starts with login into the systems and followed by choices of processes that other Public trainee has. For example, “Do Learning”, “Do assessment”, “View result”, and “Edit profile”. The differences are public administrator has more choices such as “Manage

modules”, “Manage results” and “Approve modules”. In the “Manage modules and assessments for public trainees” process, the public administrator updates and edits modules and assessments. In addition to that, the public admin also check and verify modules and assessments uploaded by public trainees in “Approve modules and assessments from public trainees” sub process. The public admin manages assessments results for Public trainee in the “Manage results for public trainees” process.

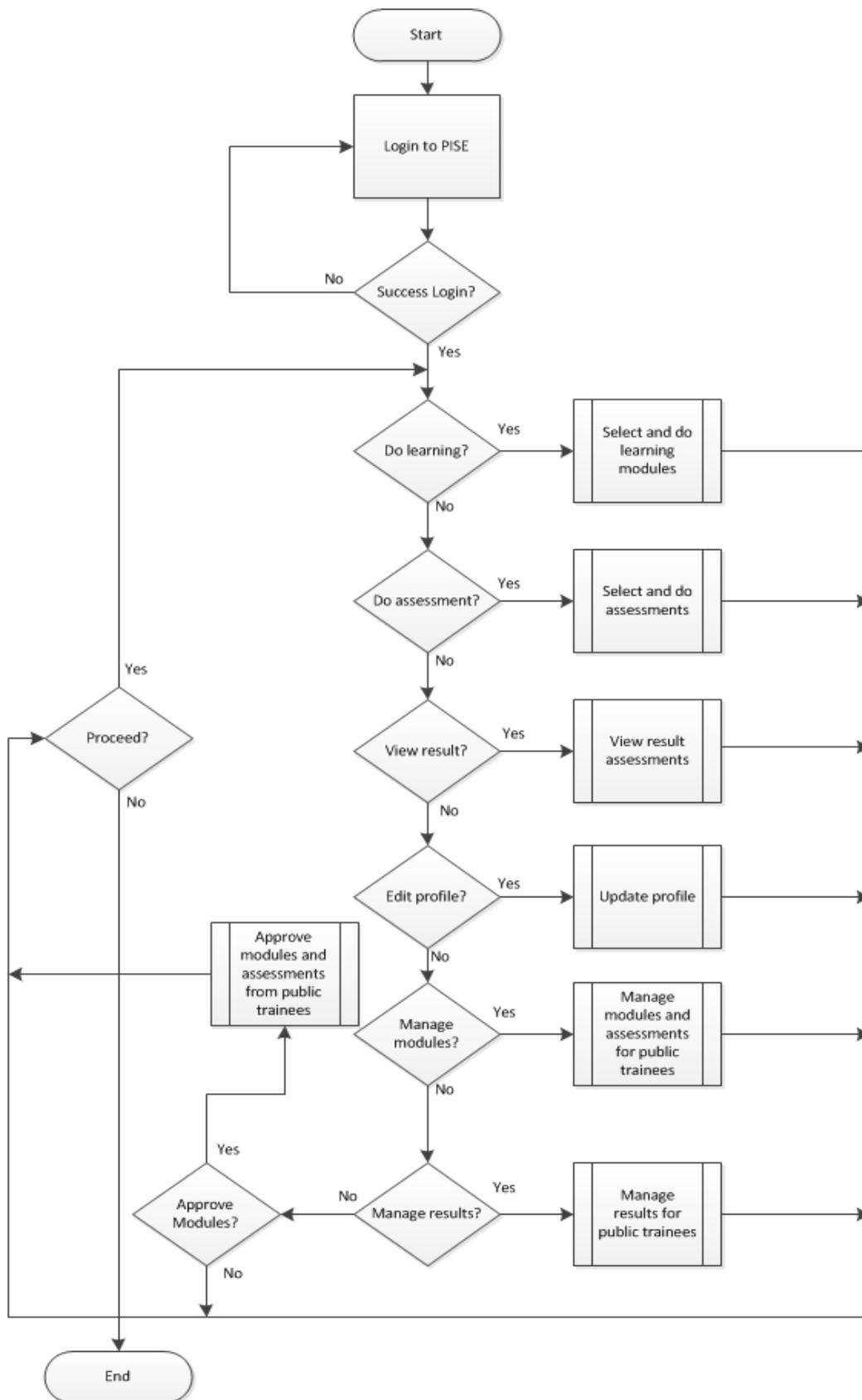


Figure 46 Flowcharts for Public PISE Training Course Administrator

The differences of the Public PISE with Private PISE are:

- a) Public PISE system could be used by anybody, and is not limited to employee in certain organisation.
- b) The syllabus, learning materials and the assessment are based upon the external organisation's learning material (e.g. ENISA/NIST). In the future, the system could have other non-profit organisation or even government organisations that are willing to provide learning materials and certification award for the Public PISE trainee.
- c) PISE has advantages as listed below:
 - i. The system is different from others because its learning materials are tailored into individual learning styles. This will make the learning process more effective and interesting. It is hoped that this will help to combat the boredom amongst the people when it comes to learning information security.
 - ii. The system has many assessments; in fact, annually assessment is recommended to ensure the user will retain information and practice what they have learnt from the training sessions. These will make individuals who use the system become knowledgeable in the security area. In the future, a certificate could be issued to the user as a form of acknowledgment for users' achievements. If the user changes organisation, he could use the certificate as proof that he is knowledgeable in the information security area.
 - iii. The system may also act as a mechanism to check current security knowledge for an individual. For example, if a user claimed that he attended many seminars on certain topics of security, then the assessment packages that related to the topics could assess and recognise his knowledge, as he claimed.
 - iv. As the system could assess individual's prior knowledge in information security, the system would not suggest the topics known to the individuals in the PLP. This will

save the individual's time, as he does not have to go through the same learning materials that he is familiar with.

- v. The system would be unique from other systems, as it provides a platform for public users to learn information security at no cost, as long as they have the Internet connection. Moreover, the public could assess their information security and would improve their security awareness, knowledge and practices without having to pay for examination fees.

6.4.3 PISE System Prototype

A simple PISE system has been created to simulate the 'look and feel' of the actual system that proposed in the previous section. In this section, the screenshots explanation is arranged based on the three types of major users of the system; trainee (Public and Private), PISE System Administrator, and Training Course Administrator (Public and Private Administrator).

6.4.3.1 Trainee (*Public and Private*)

Private and Public trainees have different registration as Private trainee will have to give details on his current organisation that he works with. See Figure 47 and Figure 48. The difference between these two trainees is, Private trainee need to key-in his position in the company and the company name. Whilst the Public trainee will only need to give the company or institution that they belongs to (if any) if not, they can still proceed with the registration. Moreover, the Public trainee does not have to obtain an approval from the PISE System Administrator to complete the registration process.

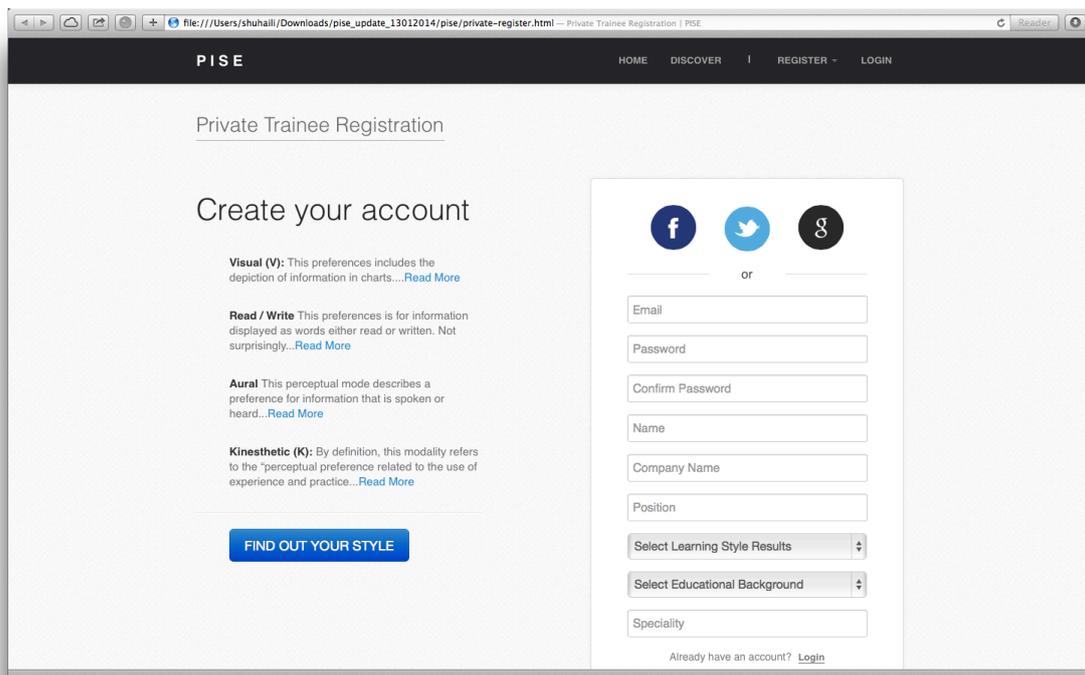


Figure 47 Screenshot for Private Trainee Registration

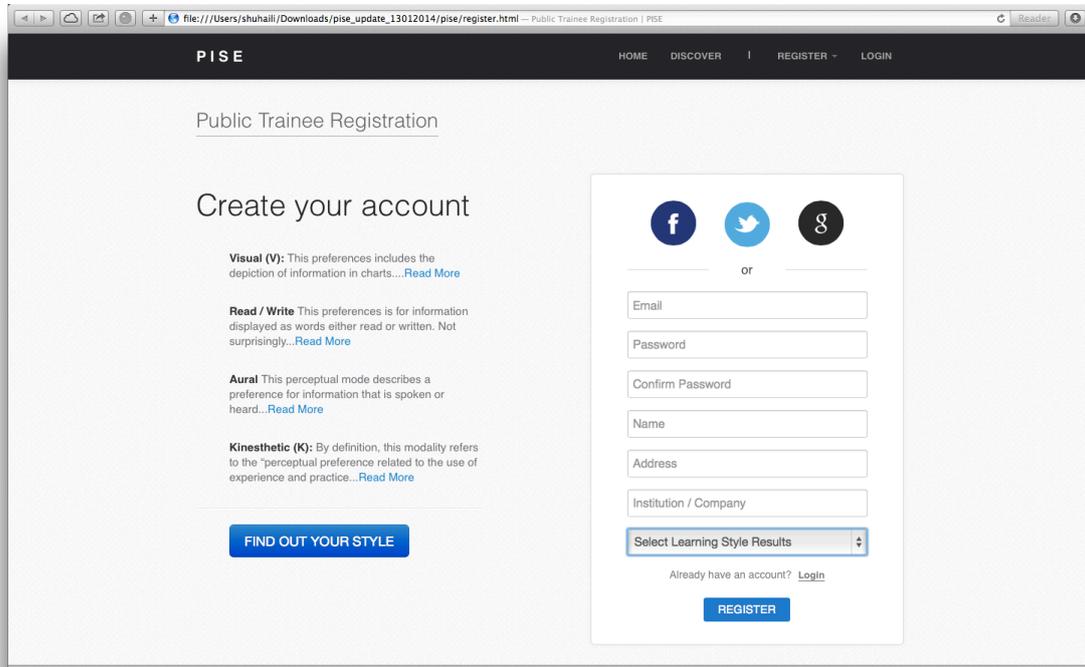


Figure 48 Screenshot for Public Trainee Registration

Once the trainee has registered to the system, he will be taking a pre-test to determine his pre-knowledge on information security. The screenshot for the trainee taking pre-test is shown in Figure 49. After the trainee completed the pre-test, the system will generate the result for the pre-test. See Figure 50. The figure also represents the way all the assessments results will be presented to the user. The graph shows the numbers of questions in the test that the trainee answered correctly or vice versa. The trainee also could view the reassessment date if they fail the previous assessment (see Figure 51).

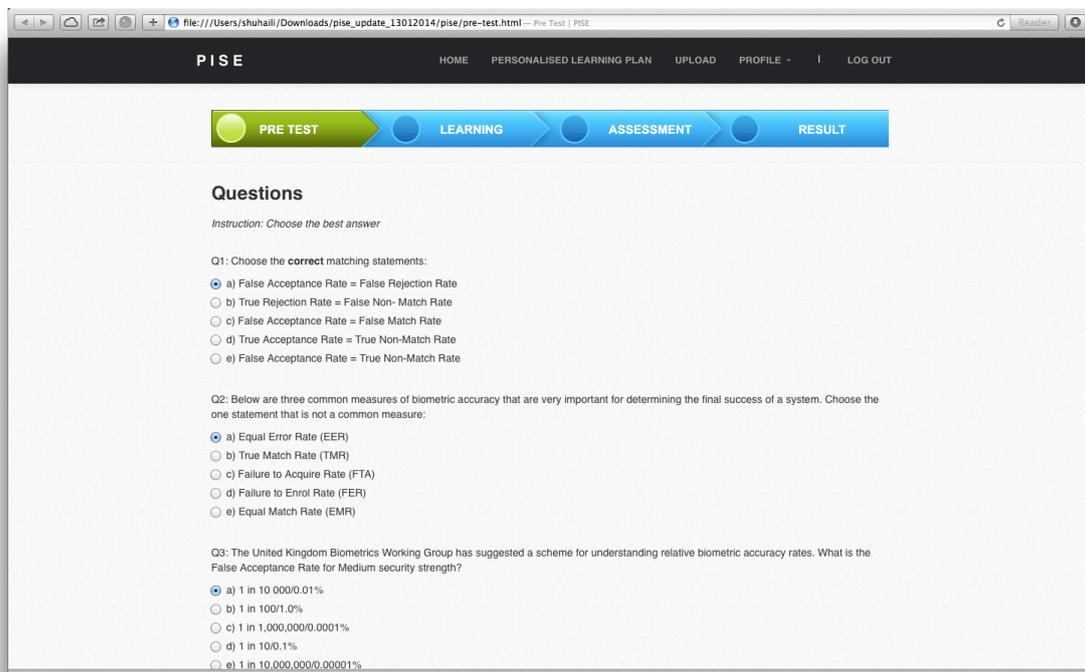


Figure 49 Screenshot for the Private and Public trainee taking pre-test

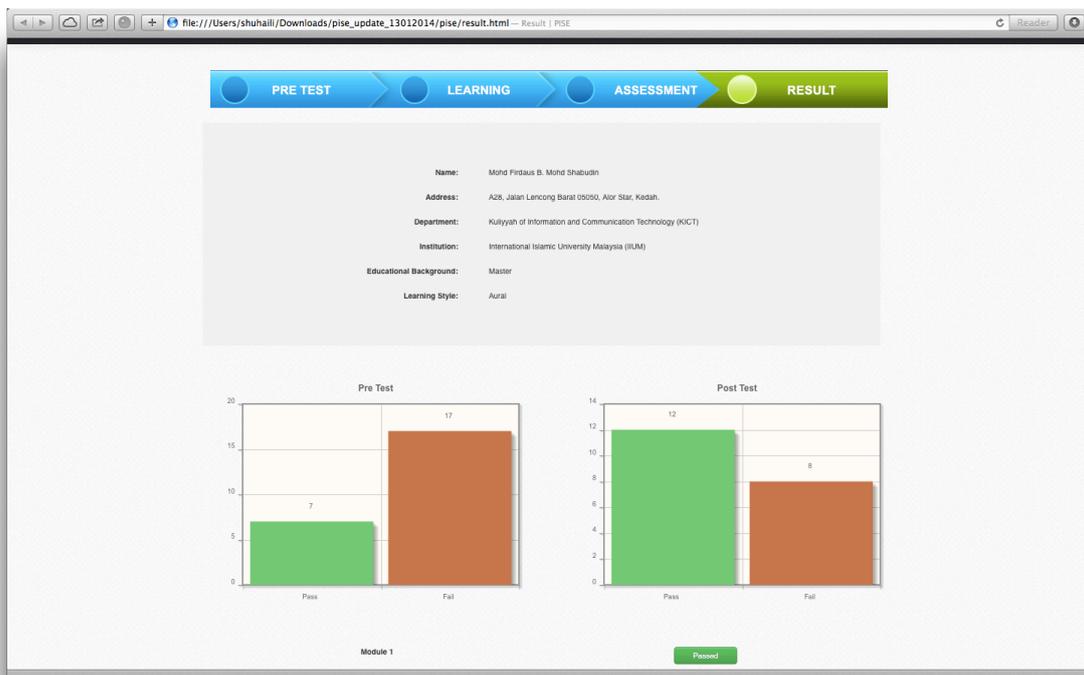


Figure 50 Screenshot for Public and Private trainee view results

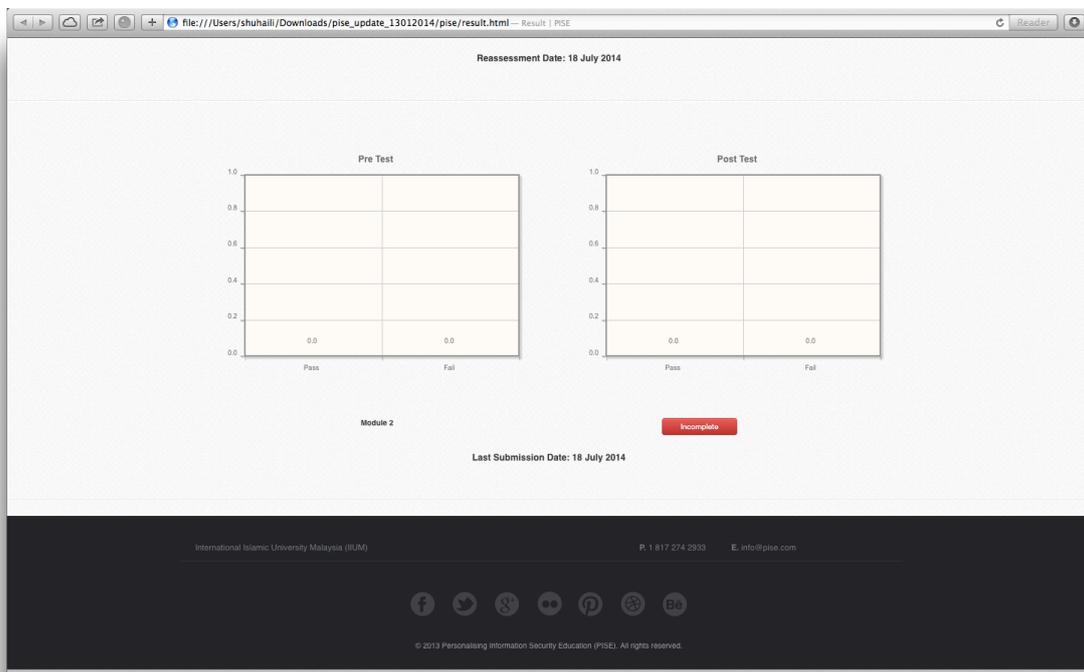


Figure 51 Screenshot for Public and Private trainee view results (continue)

The system will be able to suggest the learning materials that are suitable for the trainee based on their learning styles mode. For example, if the user is a uni-modal Visual learner,

then the system will suggest all modules for Visual learners as shown in the Figure 52 below. In the figure, the V1 is refers to Module 1 for visual learner. If the user has Visual and Aural learning styles, then the system will suggest the Module 1 – V1 or A1 (Module 1 for Aural learner).

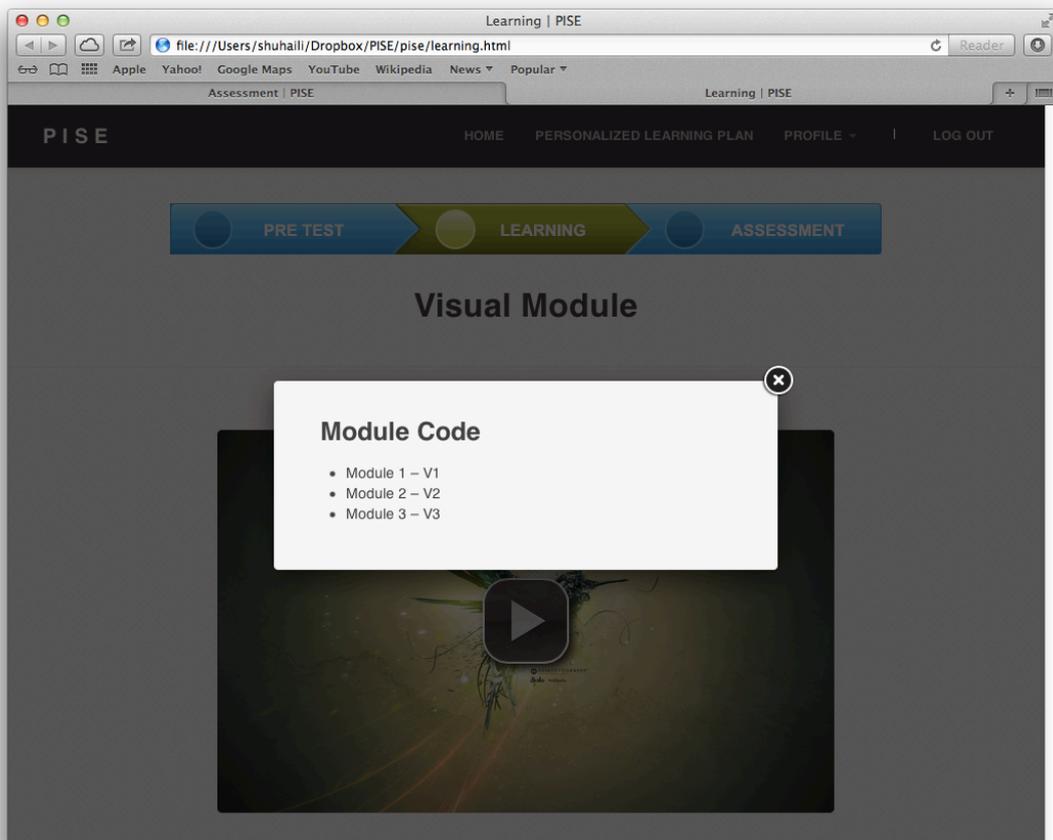


Figure 52 Screenshot for Public and Private trainee learning materials (Visual mode)

As for the visual module, the user will be able to download the materials into their machine/PC/computer as demonstrated in the Figure 53 below.

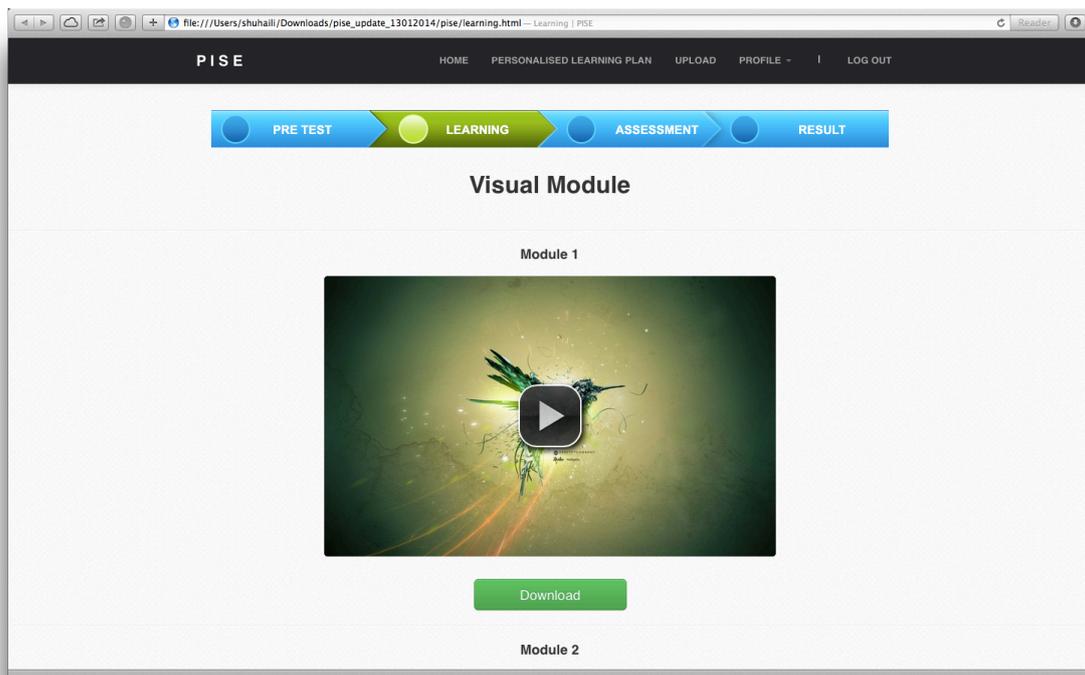


Figure 53 Screenshot for Public and Private Trainee download modules

After the trainee finishes learning process, he could choose to do the assessment for learning module that he has completed. The person could choose the assessment modules as displays in Figure 54.

Public PISE system enables their trainees to share modules and assessments to the system. Figure 55 shows the trainee could upload module and select to which learning style group it belongs to. In the screenshot, the learning styles would be VARK (see Figure 55).

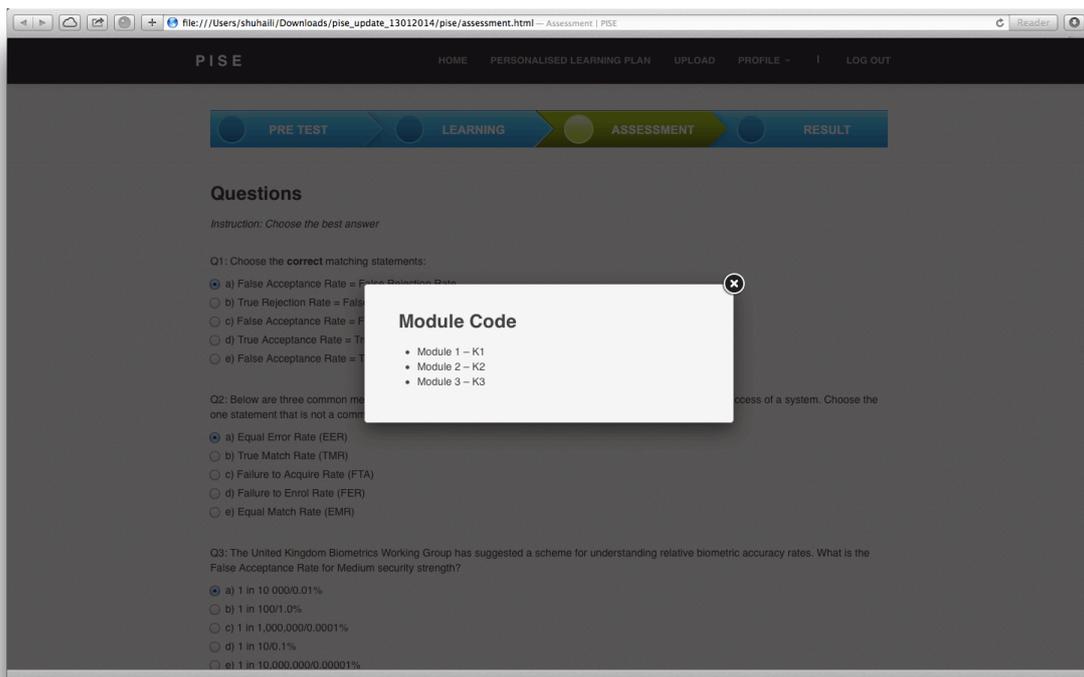


Figure 54 Screenshot for Public and Private Trainee choose assessments

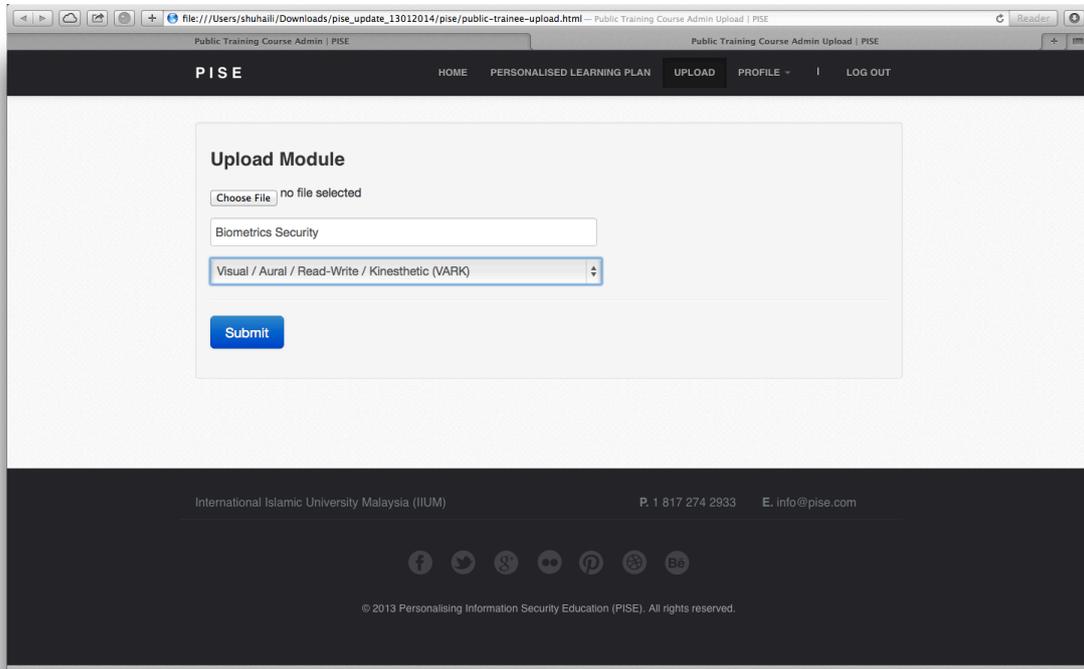


Figure 55 Screenshot for Public Trainee Upload modules

6.4.3.2 PISE System Administrator

The PISE System Administrator manages both Public and Private PISE system. Figure 56 illustrates the view of the current users in PISE system using graphs. The Private trainee registration graph (see Figure 56) shows the numbers of pending user and active users. Pending user is representing Private trainees who register to the system and waiting for the PISE System Administrator approval. The view of the verification process is presented in Figure 57. The system administrator will keep lists of employees in organisations that using Private PISE. He can approve or reject the Private trainee based on the information that he has with the information submitted by the Private trainee.

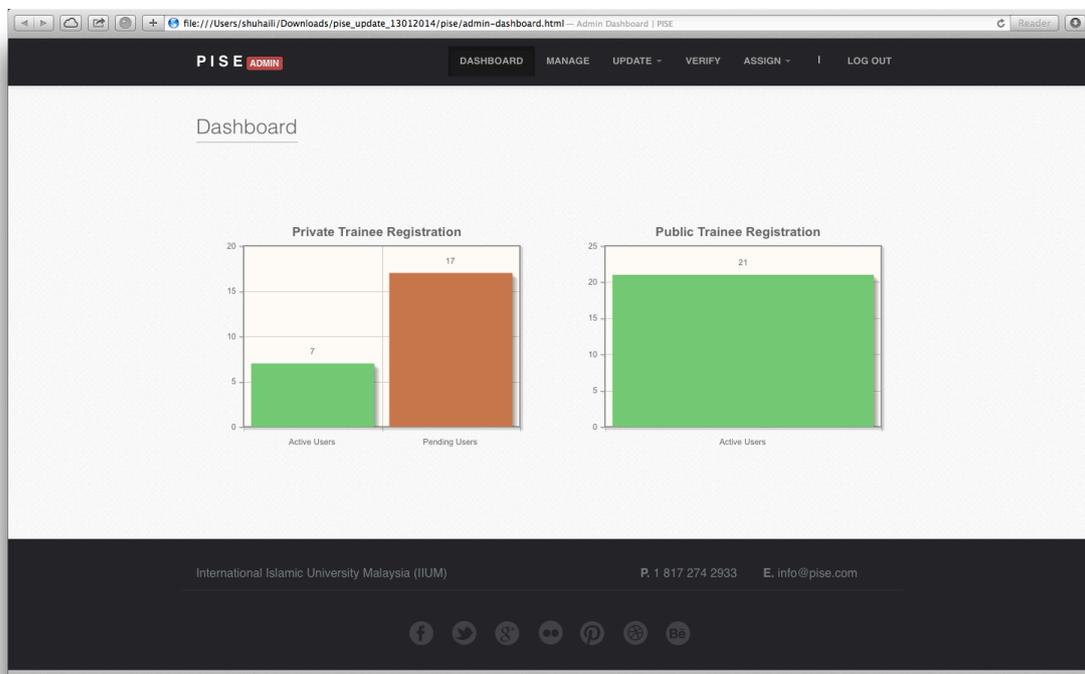


Figure 56 Screenshot for PISE System Administrator dashboard

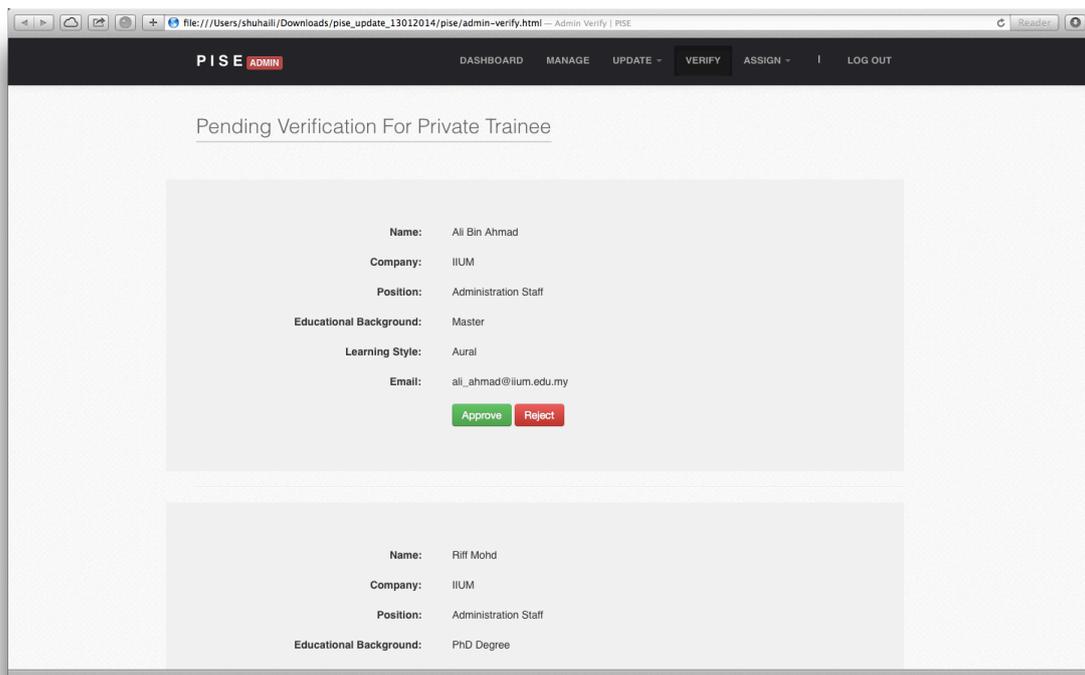


Figure 57 Screenshot for PISE System Administrator Approval

The PISE System Administrator is responsible to assign role for PISE Training Course Administrator to Public and Private trainees. In Figure 58, next to “PISE” banner, there is a word “Admin”, this is an indicator that the session is for PISE System Administrator. In the figure the admin will choose the role to be assign to the trainee. For example, if the admin would like to assign “Imran Yusof” as a “Training Course Admin” for Public PISE, he will choose the related radio button. The reason for the having the “Private Trainee” choice on the list is, there is possibilities that the Public trainee could join organisation that using Private PISE. If the system admin is to assign role to private trainee, the title “Assign Public Trainee Role: will appear as “Assign Private Trainee Role. See Figure 59.

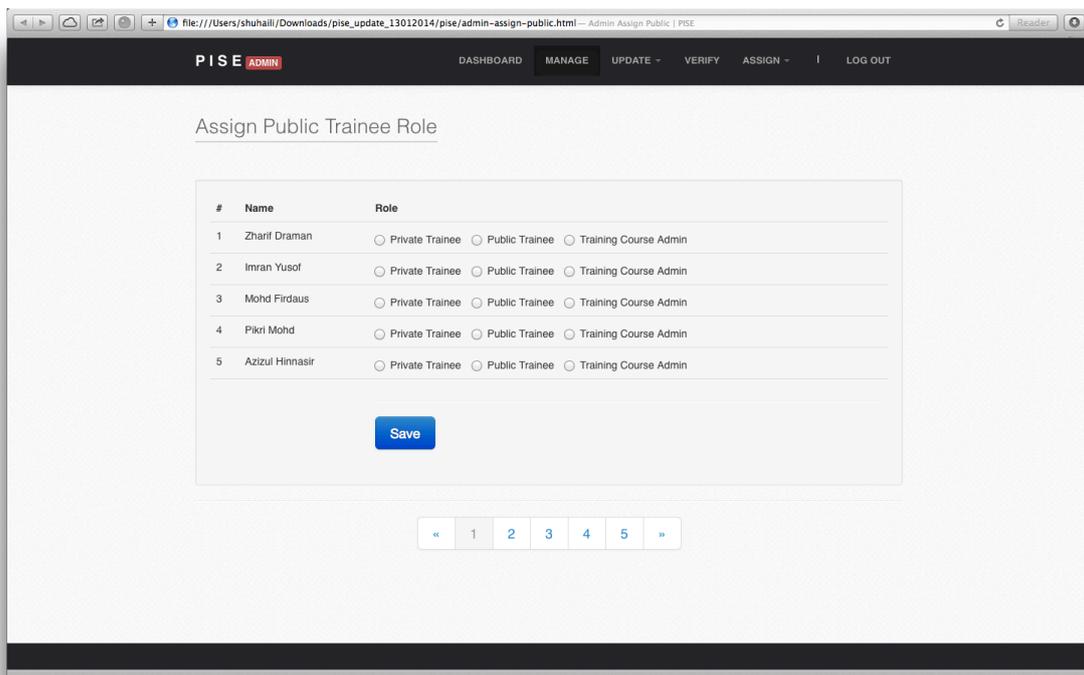


Figure 58 Screenshot for PISE System Administrator to assign role to Public trainee

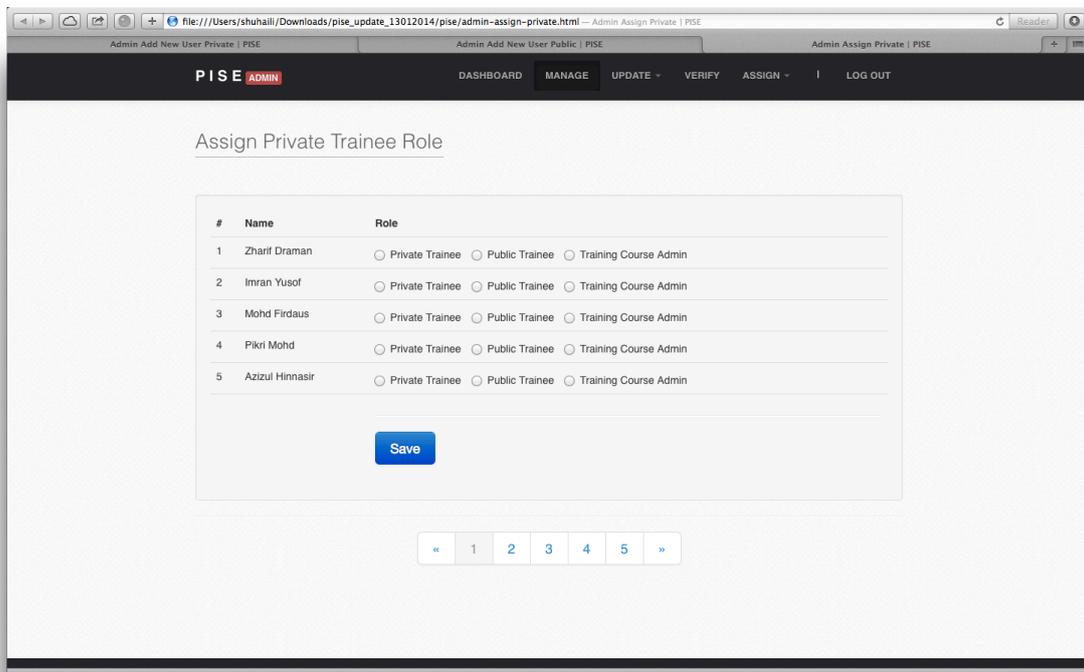


Figure 59 Screenshot for PISE System Administrator assign role to Private PISE trainee

PISE System Administrator manages trainees in the both systems (Public and Private) which demonstrated in Figure 60. The System admin could view the trainees' group. For example, "Zharif Draman" is belong to the Private PISE and "Mohd Firdaus" to the Public PISE (see Figure 60). The system admin can delete or edit all trainees in the system.

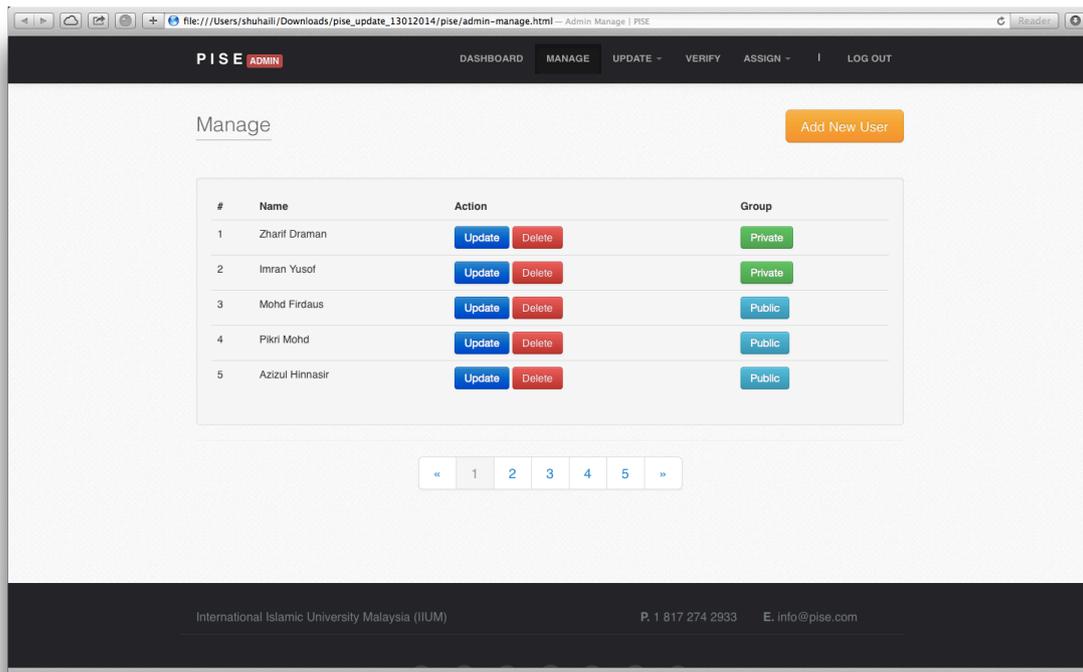


Figure 60 Screenshot for PISE System Administrator Manage trainee

6.4.3.3 Training Course Administrator (Public and Private)

The third user for PISE system is the Training Course Administrator for both Public and Private PISE. These administrators are responsible on managing modules and assessments for the respective trainees. Figure 61 illustrates the admin assigns module 2 to "Imran Yusof". The system will suggest Module 2 –K2 if Imran's learning style is Kinaesthetic. The administrator could update modules in the respective system (Public or Private PISE) such as in Figure 62. The admin can choose which modules that he would like to edit or delete. Since the Public trainees have the privilege to upload materials such as assessments,

Figure 63 demonstrates the interface for the Public PISE Training Course Administrator verifies the assessments.

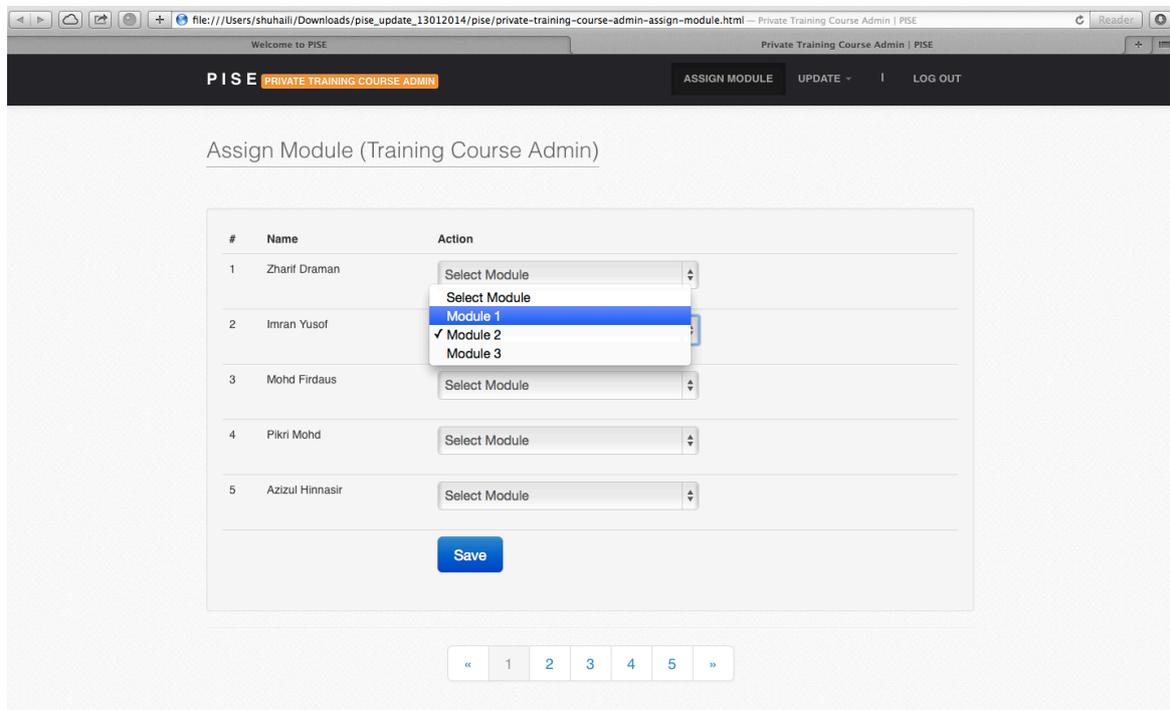


Figure 61 Screenshot for PISE Private Training Course Administrator assign module

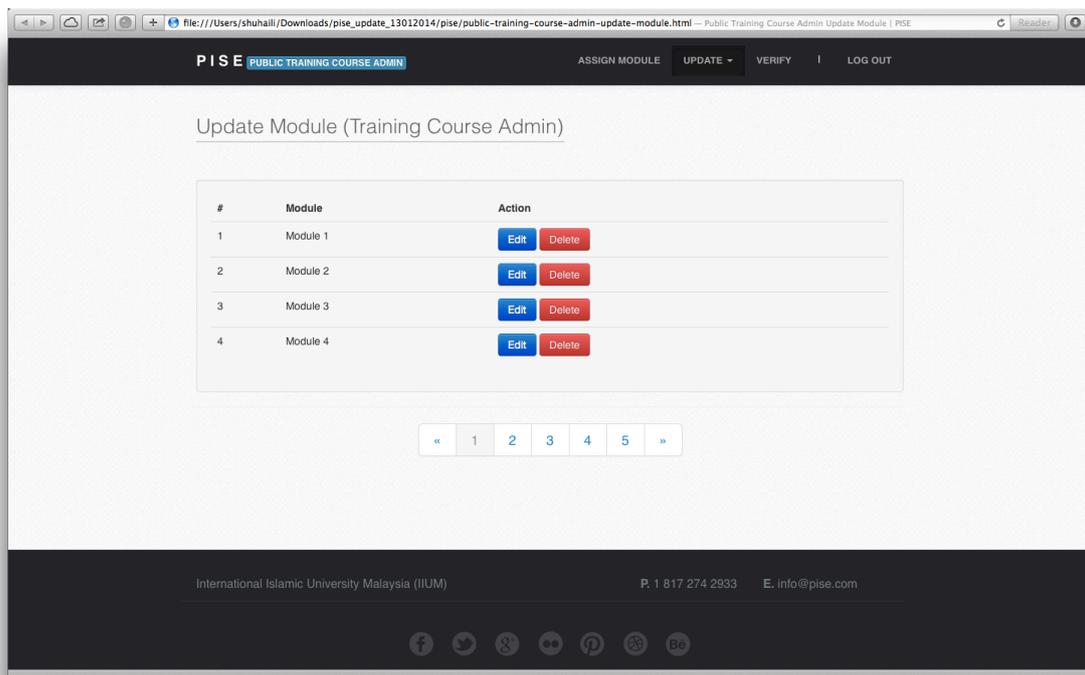


Figure 62 Screenshot for Public PISE Training Course Administrator updates module

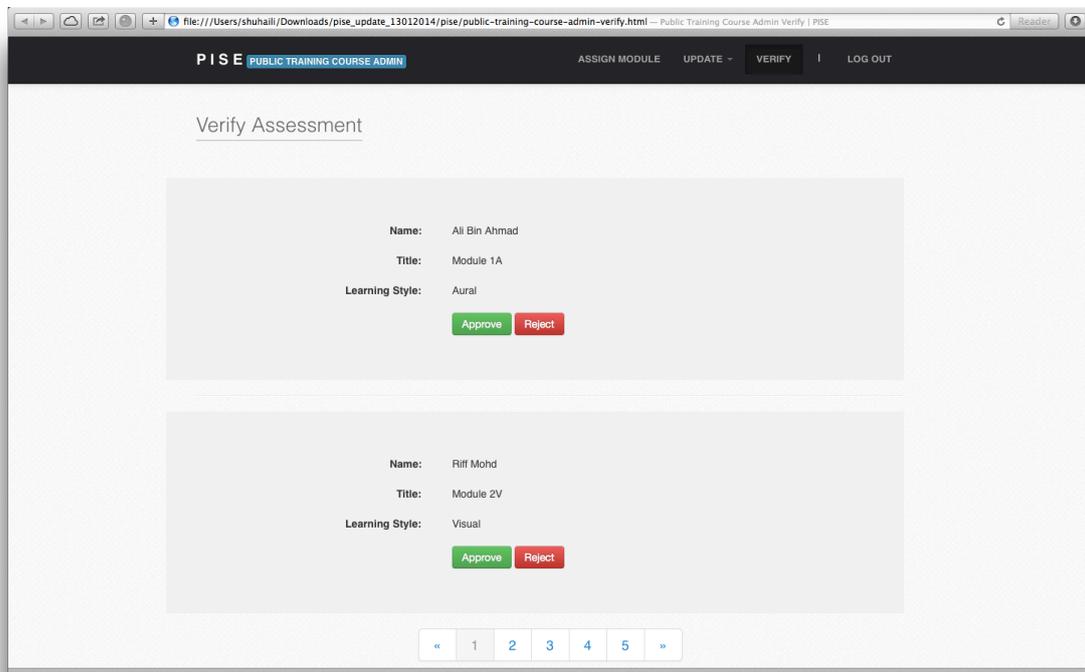


Figure 63 Screenshot for Public PISE Training Course Administrator verify assessments

6.5 PISE Evaluation and Discussion

The PISE framework is proposed to improve the learning process for information security. A prototype system for PISE was developed in order to visualise the real system of the PISE framework. An expert user was invited to evaluate the prototype and give a feedback report on the experience while using it. The feedback report is attached in the Appendix M. The expert is an associate professor who is an expert in human computer interaction. The expert has given feedback in terms of her observation on what the system could do and the interface of the system.

From the evaluation report, it has been stated that the PISE system provides clear navigation from home, pre-test, learning, assessment and finally result. Amongst the comments on her experience on testing the prototype are “The overall PISE design of the interface and navigation are easy to learn and use”. This is in line with the aim of the proposed framework to provide good experience for the future users when learning the modules.

The PISE system gives personalised learning materials to enhance the learning experiences. Therefore the system has offer a platform to the user to know their learning styles in the beginning of the registration process where the users need to do a learning styles test and provide the learning style result in the registration form. The expert user agreed that the prototype enables trainees to learn based on the learning style via the customised modules in the system.

Public PISE system enables its user not only to benefit from the customised modules, but also provide a place for sharing learning materials and assessments via upload function. The Private PISE enables the user to learn at their own time giving flexibility of learning to fulfil

the organisations requirement. The prototype demonstrates that the user could monitor their learning performance to ensure they meet the deadline for the certain module.

In the end, the expert also gave few recommendations as below:

“For enhancement, more function could be added such as email notification for verification, categorisation according to level of knowledge of the trainees (e.g. novice or expert)”.

6.6 Conclusion

The PISE framework proposed represents the two systems; Private and Public PISE. Both system support people in organisations and also the public. The Private PISE will be beneficial to employees in the organisation and the Public PISE for anybody outside the organisation.

The user of the Private trainee could also register as a Public trainee and this will enable them to upload learning materials and share their knowledge with other people in the system. The external representatives from ENISA and (ISC)² give the public trainee opportunities to learn information security from reliable sources.

The flowcharts presented in the previous section are the proposed system to give ideas on how the processes for the system might be in the future. In addition, screenshots of the PISE prototype system in this chapter demonstrates on the user interfaces while interacting with the system. The prototype presents the realisation of proposed system based on the PISE framework

In the end of the chapter, an expert evaluation on the prototype is discussed. The section provides important feedback on the usefulness of the system. However, many improvements need to be undertaken in order to have a complete training system.

The next chapter discusses the limitations and possible future work to be considered in improving the proposed framework.

7 Conclusion and Future Works

7.1 Achievements

Information security awareness and practice need improvements so that people may become more aware of the need to practice good security behaviour in their daily lives, rather than remain ignorant in these areas. To date, awareness programmes have been more about providing relevant information about improving practices, rather than ensuring that materials are suitable and effective in their task. The survey conducted in chapter 3 demonstrates that people do undertake security awareness training, and are willing to do so; however, little is known about how effective such training is. What is known, however, is that home computers remain insecure, and an attractive target for misuse. An awareness-training platform was thus proposed that provides a holistic approach to security awareness training, and provides a personalised and tailored education environment that can evaluate knowledge and skills.

In educational pedagogy, it is proven that people learn differently (Crozier, 1997; Oosterheert and Vermunt, 2001). People have their own preferences when it comes to the learning process (Heffler, 2001). There are people who like to learn in their own time, prefer to read texts rather than looking at pictures, reading a map rather than instructions. These different learning styles help people to learn in a more timely and effective manner. Hence, the PISE system has been proposed with different learning styles approaches in mind, in order to enhance learning process in information security area. It does not prescribe what these learning approaches are, but rather, presents a framework that enables relevant stakeholders to contribute learning materials in whatever form. The collaborative assessment of these resources by learners provides a simple mechanism to ensure that the most useful resources for each learning package are more readily accessible.

With regard to the objectives highlighted in Chapter 1, the achievements against each stated objective are discussed below:

a) understand the current information security awareness and practice domain

The literature review on the information security awareness and practice shows that there is a need to improve it, as it becomes an important element in human life. The current security awareness is one size fits all, and little work has been done to solve the problem.

b) from prior literature understand the issues that surround effective information security awareness

Information security awareness is aimed at improving human security behaviour. The literature indicates that human behaviour is one of the causes of information security problems. Thus, to improve security awareness, human behaviour should be improved via effective information security awareness initiatives.

c) investigate the information security awareness level of individuals within organisations and home environments

The survey results presented in chapter 3 demonstrates the level of information security awareness and practices. The survey also sought on how security behaviour in the organisations and home environments by asking the same set of questions and comparing between both context.

d) understand how individuals learn within information security training and education

The survey presented in chapter 3 also asked participants about their preferences in regards to the sources of their information security knowledge.

e) investigate models of learning and determine the role learning styles has within education

A literature survey has been done on the learning styles and personalised learning within the educational area and others.

f) to provide an empirical basis for understanding the relationship between learning styles and information security education

The study discussed in chapter 5 reveals that using learning styles in information security education does improve the learning process for the participants.

g) to propose a novel framework for personalised learning in security education

A novel framework that adopts personalised learning based on individual's learning style is proposed in chapter 6. In addition, a prototype system; PISE, which is based on the proposed framework is presented including evaluation by an expert user.in the end of the chapter.

7.2 Limitations

The research has a number of limitations arising from the fact that it was conducted by an individual researcher over a fixed timeframe. This served to limit the extent to which certain aspects could be fully realised in practice. The limitations are as below:

- 1- the initial survey in the Chapter 3 was only able to capture brief indications from each of the respondents. Other forms of interaction, such as focus groups or interviews, might give more information as to whether individuals felt that their home and workplace security practices were interrelated

- 2- the research was quantitative, and where user's experiences were captured only in terms of preferences, but without being asked whether the VARK result matched their preferences
- 3- the study on learning materials was limited to an educational organisation, and only 40 people participated in the sessions
- 4- the study only proposed the framework for the PISE system, and due to insufficient time, the implementation and the evaluation of the system in practise could not be done
- 5- PISE has many assessments to retain the employees' performance, and this may cause inconvenience to the user

7.3 Future research

In future, the systems may be improved, as per the following suggestions:

- a) A complete system based on the framework proposed could be developed and perhaps other modules related to individual personality such as personality types could be added to strengthen the learning capabilities and to ease the learning process.
- b) Based on the survey findings in chapter 3, people learn information security from informal discussions and from their colleagues and friends. Hence, an online forum could be added into the PISE system in order to enable users to discuss the topics of the materials and other information security issues.
- c) Information security practices are closely related to human behaviour. It may be that future research could collaborate the framework and system with human behaviours

elements, so as to consider motivational factors, to enhance learning process, and improve security practices.

When learning is a comfortable experience, people will be likely to learn more, and hence become better learners.

7.4 The future of information security education

Information security education should be continuous, and is not a one-time initiative. This is because information security is very much related to the technology trends, where it will grow fast from time to time. Therefore, all efforts to improve information security education should be maintained and kept updated to protect the general public.

Organisations are more aware of the importance of information security and provide security training and awareness to their employees. These are indeed good efforts in educating employees and protecting their organisations.

Whilst the general public are provided with free resources on how to protect themselves via websites and also being given awareness through media such as radio, advertisement, and television. This security awareness should be enhanced by gaining certifications to motivate the general public to keep themselves up to date with information security issues.

This research has taken into account awareness of people within organisations, and also the general public in the PISE system. It is hoped that this will contribute to the improvement of information security awareness and practices for the public user as a whole.

References

- Abbot, J. (1994), "*Learning makes sense: Recreating education for a changing future*", Letchworth: Education 2000.
- Adams, A. and Sasse, M.A. (1999), "Users are not the enemy", *Communications of the ACM*, Vol. 42 No. 12, pp. 40-46.
- Adlam, D. (2009), "Social networking identity fraud.", Available at: <http://ezinearticles.com/?Social-Networking-Identity-Fraud&id=2730177> (Accessed: 2 September 2009).
- Al-Hamdani, W.A.W.A. (2006), "Assessment of need and method of delivery for information security awareness program", *Proceedings of the Proceedings of the 2006 Information Security Curriculum Development Conference, InfoSecCD '06* Kennesaw, Georgia, USA, pp. 102-108.
- Al-Omari, A., El-Gayar, O. and Deokar, A. (2012), "Security Policy Compliance: User Acceptance Perspective", *Proceedings of the 45th Hawaii International Conference on System Sciences*, Grand Wailea, Maui, HI, USA.
- Albrechtsen, E. (2007), "A qualitative study of users' view on information security", *Computers & Security*, Vol. 26 No. 4, pp. 276-289.
- Alexandra, M.I. and Georgeta, M. (2011), "How to better meet our students' learning style through the course resources", *Annals of the University of Oradea, Economic Science Series*, Vol. 20 No. 2, pp. 578-585.
- Alkhasawneh, I.M., Mrayyan, M.T., Docherty, C., Alashram, S. and Yousef, H.Y. (2008), "Problem-based learning (PBL): Assessing students' learning preferences using vark", *Nurse Education Today*, Vol. 28, pp. 572-579.
- Almeida, V.A.F. (2012), "Privacy problems in the online world", *Internet Computing*, Vol. 16 No. 2, pp. 4-6.
- Alonso, C.M. (1993), "Educational technology and learning styles ", *Proceedings of the Tenth International Conference on Technology and Education USA*, MIT.
- Alsubaie, M. (2006), "*Creating a personalised learning environment using learning objects*", School of Construction and Property Management, University of Salford.
- Amazon.com (2012), "Amazon.co.uk", Available at: <http://www.amazon.co.uk/> (Accessed: 9 July 2012).
- APWG (2012), "*Phishing activity trends report 2nd half 2011*", Anti-Phishing Working Group (APWG). Available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2011.pdf (Accessed: 25 June 2012).

Australian Computer Emergency Response Team (2008), "Practical computer security slides", Available at: <http://www.auscert.org.au/render.html?cid=2997&it=6891> (Accessed: 8 May 2008).

Auta, E.M. (2010), "E-banking in developing economy: Empirical evidence from Nigeria", *Journal of Applied Quantitative Methods*, Vol. 5 No. 2, pp. 212-222.

Barmeyer, C.I. (2004), "Learning styles and their impact on cross-cultural training: An international comparison in France, Germany and Quebec", *International Journal of Intercultural Relations*, Vol. 28, pp. 577-594.

BERR (2008a), "Frequently asked questions", Available at: <http://www.berr.gov.uk/dius/innovation/nms/faqs/page32346.html> (Accessed: 13 November 2008).

BERR (2008b), "National minimum wage", Available at: <http://www.berr.gov.uk/employment/pay/national-minimum-wage/index.html> (Accessed: 12 May 2008).

Besnard, D. and Arief, B. (2004), "Computer security impaired by legitimate users.", *Computer & Security*, Vol. 23, pp. 253-264.

Best, B. (2007), "Practical personalised learning", Available at: <http://www.brinbest.com/id31.html> (Accessed: 26 October 2010).

Blakely, P.N. and Tomlin, A.H. (eds.) (2008) *Adult Education: Issues and Development*. New York: Nova Science Publishers, Inc.

Bojanc, R., Jerman-Blažič, B. and Tekavčič, M. (2012), "Managing the investment in information security technology by use of a quantitative modeling", *Information Processing & Management*,

Bonwell, C. and Hurd, P. (1998) 'VARK and active learning: A learning styles starter kit'. *Annual Meeting of the American Association of Higher Education* Atlanta, GA.

Boss, S., Kirsch, L., Angermeier, I., Shingler, R. and Boss, R. (2009), "If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security", *European Journal of Information Systems*, Vol. 18, pp. 151-164.

Boyle, R.A. and Dunn, R. (1998), "Teaching law students through individual learning styles", *Albany Law Review*, Vol. 62 No. 1, pp. 213-247.

Breckler, J., Joun, D. and Ngo, H. (2009), "Learning styles of physiology students interested in the health professions", *Advances in Physiology Education*, Vol. 33 No. 1, pp. 30-36.

British Broadcasting Corporation (2007), "Web networkers 'at risk of fraud'.", Available at: <http://news.bbc.co.uk/1/hi/uk/6910826.stm> (Accessed: 2 September 2009).

Brocke, J.v. and Buddendick, C. (2005), "Security awareness management - Foundations and Implementation of security awareness", *Proceedings of the 2005 International Conference on Security and Management (SAM'05)*, Las Vegas, USA.

- Burke, K. and Doolan, L.S. (eds.) (2008) *Learning styles and higher education: No adult left behind*. Adult Education: Issues and development. New York: Nova Science Publishers, Inc. 205-216 pp.
- Burton, D. (2007), "Psycho-pedagogy and personalised learning", *Journal of Education for Teaching: International research and pedagogy*, Vol. 33 No. 1, pp. 5 - 17.
- Business Enterprise Regulatory Reform (2008), "*The 9th information security breaches survey*", United Kingdom: Department for Business Enterprise and Regulatory Reform & Pricewaterhouse Coopers. 1-36 pp. Available at: http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html (Accessed: 11 May 2008).
- Cambridge University Press (2011), "Cambridge Dictionaries Online", Available at: <http://dictionary.cambridge.org/> (Accessed: 10 November 2010).
- Campbell, R.J., Robinson, W., Neelands, J., Hewston, R. and Mazzoli, L. (2007), "Personalised learning: Ambiguities in theory and practice", *British Journal of Educational Studies*, Vol. 55 No. 2, pp. 135-154.
- Cano, J.M., Garton, B.L. and Raven, M.R. (1992), "Learning styles, teaching styles and personality styles of preservice teachers of agricultural education", *Journal of Agricultural Education*, Vol. 33 No. 1, pp. 46-52.
- Carver, C.A., Jr., Howard, R.A. and Lane, W.D. (1999), "Enhancing student learning through hypermedia courseware and incorporation of student learning styles", *Education, IEEE Transactions on*, Vol. 42 No. 1, pp. 33-38.
- Cassidy, S. (2004), "Learning styles: An overview of theories, models and measures", *Educational Psychology*, Vol. 24 No. 4, pp. 419-444.
- Center for Collaborative Education (2006) *Progress and promise: Results from the Boston Pilot School January 2006*, Boston: Center for Collaborative Education.
- CERT Coordination Center Software Engineering Institute Carnegie Mellon University (2002), "Home computer security", Available at: <http://www.cert.org/homeusers/HomeComputerSecurity/#things> (Accessed: 8 May 2008).
- Chapin, N. (1979), "Full report of the Flowchart Committee on ANS Standard X3.5-1970", *ACM SIGPLAN Notices*, Vol. 14 No. 3, pp. 16-27.
- Chen, C.C., Medlin, B.D. and Shaw, R.S. (2008), "A cross-cultural investigation of situational information security awareness programs", *Information Management & Computer Security*, Vol. 16 No. 4, pp. 360-376.
- Chia, P.A., Maynard, S.B. and Ruighaver, A.B. (2002), "Understanding organizational security culture", *Proceedings of the Sixth Pacific Asia Conference on Information Systems* Tokyo, Japan, pp. 731-740.
- Clark, C. and Rumbold, K. (2006) *Reading for pleasure: A research overview*. National Literacy Trust. [Online]. Available at: http://www.scholastic.com/teachers/article/collateral_resources/pdf/i/Reading_for_pleasure.pdf (Accessed: 12 May 2012).

- Coffield, F., Moseley, D., Hall, E. and Ecclestone, K. (2004a) 'Families of learning styles'. [Learning and Skills Research Centre].
- Coffield, F., Moseley, D., Hall, E. and Ecclestone, K. (2004b), "*Learning styles and pedagogy in post-16 learning: A systematic and critical review*", Wiltshire: Learning and Skills Development Agency.
- Coman, M.J. and Heavers, K.L. (1998), "*How to improve your study skills*", 2nd edition, Lincolnwood, Illinois: NTC Publishing.
- comScore MMX (2012), "1 in 4 Internet users access banking sites globally", Available at: <http://www.comscoredatamine.com/2012/06/1-in-4-internet-users-access-banking-sites-globally/> (Accessed: 9 July 2012).
- Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D. (2007), "A video game for cyber security training and awareness", *Computers & Security*, Vol. 26 No. 1, pp. 63-72.
- Conklin, W.R., White, G.B., Cothren, C., Williams, D. and Davis, R.L. (2005), "*Principles of computer security: Security+ and beyond*", United States: McGraw-Hill Companies.
- Cook, D.M., Szewczyk, P. and Sansurooah, K. (2011), "Securing the elderly: A developmental approach to hypermedia based online information security for senior novice computer users", *Proceedings of the 2nd International Cyber Resilience Conference*, Perth, Western Australia.
- Cooper, M.H. (2008) 'Information security training: lessons learned along the trail'. *Proceedings of the 36th annual ACM SIGUCCS conference on User services conference*. Portland, OR, USA: ACM.
- Courcier, I. (2007), "Teacher's perceptions of personalised learning", *Evaluation & Research in Education*, Vol. 20 No. 2, pp. 59-80.
- Crowley, E. (2004), "Experiential learning and security lab design", *Proceedings of the CITC5 '04 Proceedings of the 5th conference on Information technology education*, Salt Lake City, Utah, USA, pp. 169-176.
- Crozier, W.R. (1997), "*Individual learners: Personality differences in education*", New York: Routledge.
- Cutler, T., Waine, B. and Brehony, K. (2007), "A new epoch of individualization? Problems with the personalization of public sector services", *Public Administration*, Vol. 85 No. 3, pp. 847-855.
- Cyber Crime Watch (2011), "Cyber Crime Statistics", Available at: <http://www.cybercrimeswatch.com/cyber-crime/cyber-crime-statistics.html> (Accessed: 7 July 2012).
- Dainton, S. (2004), "Personalised learning", *Symposium Journals 2004*, Vol. 46 No. 2, pp. 56-58.
- Davis, S.E. (2007), "Learning styles and memory", *Institute for Learning Styles Journal*, Vol. 1, pp. 46-51.

Dembo, M.H. and Howard, K. (2007), "Advice about the use of learning styles: A major myth in education", *Journal of College Reading and Learning*, Vol. 37 No. 2, pp. 101-109.

Department for Children School and Families (2010), "Personalised learning approaches used by schools", Available at: <http://www.dcsf.gov.uk/research/programmeofresearch/projectinformation.cfm?projectId=14664&type=5&resultspage> (Accessed: 6 May 2010).

Department for Education (2010), "The national strategies", Available at: <http://nationalstrategies.standards.dcsf.gov.uk/node/83603> (Accessed: 4 November 2010).

Diehl, G.E. and Doucette, R. (1999), "Why have four-option multiple choice questions?", Navy Education and Training 1-5 pp. Available at: <http://www.dtic.mil/docs/citations/ADA362211> (Accessed: 2 August 2011).

Diehl, V.A. (2004), "Access to affordances, development of situation models, and identification of procedural text problems", *Professional Communication, IEEE Transactions on*, Vol. 47 No. 1, pp. 54-64.

Dlamini, M.T., Eloff, J.H.P. and Eloff, M.M. (2009), "Information security: The moving target", *Computers & Security*, Vol. 28 No. 3-4, pp. 189-198.

Doherty, B.C., O'Hare, P.T., O'Grady, M.J. and O'Hare, G.M.P. (2006), "Entre-pass: Personalising u-learning with Intelligent Agents", *Proceedings of the International Workshop on Wireless, Mobile and Ubiquitous Technology in Education (ICHIT'06)*, Jeju Island, Korea.

Dunn, R. (1984), "Learning styles: State of the science", *Theory into Practice*, Vol. 23 No. 1, pp. 10-19.

Dunn, R. and Dunn, K. (1978), "Teaching students through their individual learning styles : A practical approach", Reston Publishing Company.

Durán, E.B. and Amandi, A. (2009), "Personalised collaborative skills for student models", *Interactive Learning Environments*, Vol. First published on: 15th January 2009 (iFirst),

Earley, C. and Ang, S. (2003), "Cultural intelligence: Individual interactions across cultures", Palo Alto, CA: Stanford Business Books.

El-Haddadeh, R., Tsohou, A. and Karyda, M. (2012), "Implementation challenges for information security awareness initiatives in E-government", *Proceedings of the European Conference on Information Systems (ECIS)*, Barcelona, Spain.

ENISA (2007), "Information security awareness: Local government and Internet service providers", Available at: http://www.enisa.europa.eu/doc/pdf/deliverables/inf_sec_aware_init_local_gov_isps_19102007.pdf (Accessed: 4 November 2008).

Entwisle, N. (2001), "Styles of learning and approaches to studying in higher education", *Kybernetes*, Vol. 30 No. 5/6, pp. 593-602.

European Network and Information Security Agency (2008), "The new users' guide: How to raise information security awareness", European Network and Information Security Agency. 99 pp. Available at: <http://www.ifap.ru/library/book327.pdf> (Accessed: 15 September 2008).

- Felder, R.M. and Silverman, L.K. (1988), "Learning and teaching styles in engineering education", *Engineering Education*, Vol. 78 No. 7, pp. 674-681.
- Felder, R.M. and Soloman, B.A. (2009), "Learning styles and strategies", Available at: <http://www4.ncsu.edu/unity/lockers/users/f/felder/public/ILSdir/styles.htm> (Accessed: 13 October 2009).
- Fleming, N.D. (2001), "The VARK Questionnaire ", Available at: <http://www.vark-learn.com/english/page.asp?p=questionnaire> (Accessed: 1 August 2011).
- Fleming, N.D. (2006), "*Teaching and learning styles: VARK strategies*", Second edition, Christchurch, New Zealand: Neil D Fleming.
- Fleming, N.D. (2011a), "Feedback: What people say about VARK", Available at: <http://www.vark-learn.com/english/page.asp?p=testimonials> (Accessed: 16th May 2012).
- Fleming, N.D. (2011b), "Research & statistics", Available at: <http://www.vark-learn.com/english/page.asp?p=research> (Accessed: 10 May 2012).
- Fleming, N.D. and Bonwell, C.C. (2001), "VARK: A guide to learning styles", Available at: <http://www.vark-learn.com> (Accessed: 15 October 2010).
- French, G., Cosgriff, T. and Brown, T. (2007), "Learning style preferences of Australian occupational therapy students", *Australian Occupational Therapy Journal*, Vol. 54, pp. 58-65.
- Furnell, S. and Evangelatos, K. (2007), "Public awareness and perceptions of biometrics", *Computer Fraud & Security*, Vol. 2007 No. 1, pp. 8-13.
- Furnell, S. and Thomson, K.-L. (2009), "From culture to disobedience: Recognising the varying user acceptance of IT security", *Computer Fraud & Security*, Vol. 2009 No. 2, pp. 5-10.
- Gardner, H. (1993), "*Multiple intelligences: The theory in practice*", New York: Basic Books.
- Garton, L., Haythornthwaite, C. and Wellman, B. (eds.) (1999) *Studying on-line social networks* Doing internet research: Critical issues and methods for examining the net. Thousand Oaks, CA: Sage.
- Gentry, P. (1990), "*Learning styles and culture: A practical application*", Notes on Literacy. vol. 62.
- GetNetWise (2008), "Security tips", Available at: <http://security.getnetwise.org/tips/> (Accessed: 10 May 2012).
- GetSafeOnline (2009), "Get safe online with free, expert advice.", Available at: <http://www.getsafeonline.org/> (Accessed: 23 July 2009).
- Gilbert, C. (2007), "*2020 Vision: Report on the teaching and learning in 2020 review group*". Available at: <http://publications.teachernet.gov.uk/eOrderingDownload/6856-DfES-Teaching%20and%20Learning.pdf> (Accessed: 22 March 2010).
- Gilbert, J.E. and Swanier, C.A. (2008), "Learning styles: How do they fluctuate?", *Institute for Learning Styles Journal*, Vol. 1, pp. 29-40.

- Gonzalez, J.J. and Sawicka, A. (2002), "A framework for human factors in information security", *Proceedings of the Proceedings of 2002 WSEAS Int. Conf. on Information Security*, Rio de Janeiro.
- Graham, C. (2010), "*Personal information online code of practice*", Cheshire, UK: Information Commissioner's Office. Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_information_online_cop.pdf (Accessed: 2 July 2011).
- Grant, I. (2007), "DaimlerChrysler security drive targets 360,000 staff", Available at: <http://www.computerweekly.com/Articles/2007/10/12/227469/daimlerchrysler-security-drive-targets-360000-staff.htm> (Accessed: 4 November 2008).
- Grasha, A. (1996), "*Teaching with Style: A practical guide to enhancing learning by understanding teaching & learning styles*", Pittsburgh: Alliance Publishers.
- Gregorc, A.F. (1979), "Learning/teaching styles: Potent forces behind them ", *Educational Leadership*, Vol. 36 No. 4, pp. 234-236.
- Guldberg, H. (2004) 'Class divisions: Who benefits from the 'personalised learning' strategy of dividing school pupils into sub-sets?'. [Online]. Available at: <http://www.spiked-online.com/site/article/2329/>.
- Hargreaves, C. and Prince, D. (2013), "*Understanding Cyber Criminals and Measuring Their Future Activity*", Lancaster University. Available at: http://eprints.lancs.ac.uk/65477/1/Final_version_Understanding_cyber_criminals_and_measuring_their_activity.pdf (Accessed: 10 January 2014).
- Hargreaves, D.H. (2006), "A new shape for schooling?", Available at: http://curriculumdesign.ssatrust.org.uk/8dR356im/1247-29072009-1124-2c-01%20a%20new%20shape%20for%20schooling_128414.pdf (Accessed: 2 December 2010).
- Harris Interactive (2009), "Online security and privacy study.", Available at: <http://staysafeonline.mediaroom.com/index.php?s=67> (Accessed: 23 July 2009).
- Hawk, T.F. and Shah, A.J. (2007), "Using Learning Style Instruments to Enhance Student Learning", *Decision Sciences Journal of Innovative Education*, Vol. 5 No. 1, pp. 1-19.
- Hawkins, S., Yen, D.C. and Chou, D.C. (2000), "Awareness and challenges of Internet security", *Information Management & Computer Security*, Vol. 8 No. 3, pp. 131-143.
- Hayes, J. and Allinson, C.W. (1988), "Cultural differences in the learning styles of managers", *Management International Review*, Vol. 28 No. 75-80,
- Heffler, B. (2001), "Individual Learning Style and the Learning Style Inventory", *Educational Studies*, Vol. 27 No. 3, pp. 307 - 316.
- Herlihy, C.M. and Kemple, J.J. (2004), "*The Talent Development High School Model: Context, components, and initial impacts on students' performance and attendance* ", MDRC.
- Herold, R. (2005), "*Managing an information security and privacy awareness and training program*", CRC Press.

- Hinde, S. (2004), "Hacking gains momentum", *Computer Fraud & Security*, Vol. 2004 No. 11, pp. 13-15.
- Honey, P. and Mumford, A. (1992), *The manual of learning styles*, Maidenhead: Peter Honey.
- Honey, P. and Mumford, A. (2006), *The learning styles questionnaire 80-item version*, Maidenhead: Peter Honey Publications.
- Hunter, P. (2008), "Social networking: the focus for new threats -- and old ones", *Computer Fraud & Security*, Vol. 2008 No. 7, pp. 17-18.
- Husen, T. and Postlethwaite, T.N. (eds.) (1994) *Instructional design models*. 2nd edn. The International Encyclopedia of Education Oxford, UK: Pergamon.
- Hyland, K. (1993), "Culture and learning: A study of the learning style preferences of Japanese students", *RELC Journal*, Vol. 24 No. 2, pp. 69-91.
- IBM Corporation (1970), "Flowcharting Techniques", Available at: <http://www.fh-jena.de/~kleine/history/software/IBM-FlowchartingTechniques-GC20-8152-1.pdf> (Accessed: 17 January 2014).
- Inglesant, P. and Sasse, M.A. (2011), "Information security as organizational power: A framework for re-thinking security policies", *Proceedings of the Socio-Technical Aspects in Security and Trust (STAST) 2011* Milan, Italy, pp. 9-16.
- Internet Safety Zone (2012), "Online safety advice by the University of Central Lancashire", Available at: <http://www.internetsafetyzone.co.uk/> (Accessed: 10 May 2012).
- Jacobson, I., Christerson, M., Jonsson, P. and Övergaard, G. (1992), *Object-Oriented Software Engineering - A Use Case Driven Approach*, Addison-Wesley.
- Jain, D., Krishna, P.V. and Saritha, V. (2012) 'A study on Internet of Things based applications'. [Online]. Available at: <http://arxiv.org/pdf/1206.3891v1> (Accessed: 11 July 2012).
- James, S., D'amore, A. and Thomas, T. (2011), "Learning preferences of first year nursing and midwifery students: Utilising VARK", *Nurse Education Today*, Vol. 31, pp. 417-423.
- James, W. and Gardner, D. (1995), "Learning styles: Implications for distance learning", *New Directions for Adult and Continuing Education*, Vol. 67,
- Jenkins, C. (2005), *Skills for success: Developing effective study strategies*, Belmont, CA: Wadsworth/Thompson Learning.
- Jenkins, J.M. and Keefe, J.W. (2002), "Two schools: Two approaches to personalized learning", *Phi Delta Kappan*, Vol. 83 No. 6, pp. 449-456.
- Johnson, M. (2004a), "Personalised learning - An emperor outfit?", Available at: <http://www.ippr.org.uk/uploadedFiles/research/projects/Education/Personalised%20Learning.pdf> (Accessed: 6 May 2010).

- Johnson, M.E. (2004b), "Personalised learning: New directions for schools?", *New Economy*, Vol. 11 No. 4, pp. 224-228.
- Jones, A. (2008), "The changing nature of malicious attacks", *Computer Fraud & Security*, Vol. 2008 No. 6, pp. 15-17.
- Jones, P. and Burns, M. (2006), "*Personalising learning: How to transform learning through system wide reform*", Stafford: Network Continuum Education
- Kalkan, M. (2008), "Learning preferences and problem-based discussion sessions: A study with Turkish maritime students", *Social Behavior and Personality*, Vol. 36 No. 10, pp. 1295-1302.
- Kanar, C.C. (1995), "*The confident student*", Boston: Houghton Mifflin Company.
- Karim, N.S.A. and Hasan, A. (2007), "Reading habits and attitude in the digital age: Analysis of gender and academic program differences in Malaysia", *The Electronic Library*, Vol. 25 No. 3, pp. 285-298.
- Karjalainen, M. and Siponen, M. (2011), "Toward a new meta-theory for designing information systems (IS) security training approaches", *Journal of the Association for Information Systems*, Vol. 12 No. 8, pp. 518-555.
- Karmeshu, Raman, R. and Nedungadi, P. (2012), "Modelling diffusion of a personalized learning framework", *Educational Technology Research Development*, No. Special issue on personalized learning,
- Kelley, S. (2008), "Course description: Computer and network security awareness ", Available at: <http://www.sans.org/training/description.php?mid=90> (Accessed: 7 May 2008).
- Khan, B., Alghathbar, K.S., Nabi, S.I. and Khan, M.K. (2011), "Effectiveness of information security awareness methods based on psychological theories", *African Journal of Business Management*, Vol. 5 No. 26, pp. 10862-10868.
- Kim, B. and Chris, S. (2001), "Accommodating diverse learning style in the design and delivery of on-line learning experiences", *International Journal of Engineering*, Vol. 17, pp. 93-98.
- Kim, D.H. (1998), "The link between individual and organizational learning", Available at: <http://books.google.co.uk/books?id=tOjleHACgiMC&lpg=PA41&ots=-dnjZhXyQT&dq=learning%20theories%20related%20to%20individual%20learning&lr&pg=PA41#v=onepage&q&f=false> (Accessed: 4 October 2010).
- Kinshuk and Taiyu Lin (2003) 'Application of learning styles adaptivity in mobile learning environments'. *ASEE Annual Conference and Exposition* Nashville, Tennessee: 23-25 June 2003.
- Knowles, M.S. (1988), "*The modern practice of adult education, from pedagogy to andragogy: Revised and updated*", Englewood Cliffs, NJ: Cambridge Adult Education.
- Koch, J., Salamonson, Y., Rolley, J.X. and Davidson, P.M. (2011), "Learning preference as a predictor of academic performance in first year accelerated graduate entry nursing students: A prospective follow-up study", *Nurse Education Today*, Vol. 31, pp. 611-616.

- Kolb, D. (2000), "*Facilitator's guide to learning*", Boston: Hay/McBer.
- Kolb, D.A. (1981), "Learning styles and disciplinary differences", Available at: <http://www.learningfromexperience.com/images/uploads/Learning-styles-and-disciplinary-difference.pdf> (Accessed: 13 October 2009).
- Kolb, D.A. (1984), "*Experiential learning: Experience as the source of learning and development*", Upper Saddle River, NJ: Prentice-Hall.
- Kovalchick, A. and Dawson, K. (eds.) (2003) *ADDIE Model*. Educational Technology: An Encyclopedia. Santa Barbara, CA: ABC-Clio.
- Kratzig, G. and Arbuthnott, K. (2003), "Perceptual learning style and learning proficiency: A test of the hypotheses", *Journal of Educational Psychology*, Vol. 98 No. 1, pp. 1-16.
- Kritzinger, E. and Smith, E. (2008), "Information security management: An information security retrieval and awareness model for industry", *Computers & Security*, Vol. 27 No. 5-6, pp. 224-231.
- Kritzinger, E. and von Solms, S.H. (2010), "Cyber security for home users: A new way of protection through awareness enforcement", *Computers & Security*, Vol. 29, pp. 840-847.
- Kruger, H.A. and Kearney, W.D. (2006), "A prototype for assessing information security awareness", *Computers & Security*, Vol. 25 No. 4, pp. 289-296.
- Krutz, R.L. and Vines, R.D. (2007), "*The CISSP and CAP Pre Guide: Platinum Edition*", Indianapolis, USA: Wiley Publishing.
- Lacey, D. (2010), "Understanding and transforming organizational security culture", *Information Management & Computer Security*, Vol. 18 No. 1, pp. 4-13.
- Lahey, B.B. (2004), "*Psychology: An introduction*", 8th edition, Boston: McGraw Hill.
- Leadbeater, C. (ed.) (2006) *The future of public services: Personalised learning*. Schooling for Tomorrow: Personalising Education. Paris: OECD.
- Leite, W.L., Svinicki, M. and Shi, Y. (2010), "Attempted validation of the scores of the VARK: Learning styles inventory with multitrait-multimethod confirmatory factor analysis models", *Educational and Psychological Measurement*, Vol. 70, pp. 323-339.
- Litan, A. (2004), "*Phishing attack victims likely targets for identity theft*", Gartner Research. Available at: http://www.gartner.com/resources/120800/120804/phishing_attack.pdf (Accessed: 12 August 2008).
- Liu, M. and Chen, L. (2008), "Personalized learning system based on Solomon Learning Style", *IEEE Computer Society*, Vol. 5, pp. 820-823.
- Lujan, H.L. and DiCarlo, S.E. (2006), "First year medical students prefer multiple learning styles", *Advances in Physiology Education*, Vol. 30 No. 1, pp. 13-16.
- Luo, X., Brody, R., Seazzu, A. and Burd, S. (2011), "Social engineering: The neglected human factor for information security management", *Information Resources Management Journal*, Vol. 24 No. 3, pp. 8.

- Maguire, A. (2008), "Achieving real personalised learning: Considerations on blended learning", Available at: http://www.thirdforce.com/resources/whitepaper/WP_AMaguire01.pdf (Accessed: 30 March 2010).
- Mahabi, V. (2010) *Information security awareness: System administrators and end-user perspectives* Electronic Thesis. Florida State University.
- Mahony, P. and Hextall, I. (2009), "Building schools for the future and the implications for becoming a teacher", *Proceedings of the European Conference on Educational Research*, Vienna.
- Mann, I. (2008), "Hacking the human [IT Security]", *Engineering and Technology*, Vol. 3 No. 1, pp. 62-63.
- Martin, E. (2009), "What do flowchart symbols mean?", Available at: http://www4.uwsp.edu/geo/faculty/gmartin/geog476/Lecture/flowchart_symbols.html (Accessed: 17 January 2014).
- Martinez, M. (2002), "Designing learning objects to personalize learning", Available at: <http://www.reusability.org/read/chapters/martinez.doc> (Accessed: 23 February 2009).
- Materna, L. (2007), *Jump Start the Adult Learner: How to Engage and Motivate Adults Using Brain-Compatible Strategies*, California, US: Corwin Press.
- Maxion, R.A. and Reeder, R.W. (2005), "Improving user-interface dependability through mitigation of human error.", *International Journal of Human Computer Studies*, Vol. 63 No. 1-2, pp. 25-50.
- May, C. (2008), "Approaches to user education", *Network Security*, Vol. 2008 No. 9, pp. 15-17.
- McAfee (2009), "McAfee security tips - 13 ways to protect your system", Available at: http://www.mcafee.com/us/threat_center/tips.html (Accessed: 2 September 2009).
- McCoy, C. and Fowler, R.T. (2004) "'You are the key to security': establishing a successful security awareness program". *Proceedings of the 32nd annual ACM SIGUCCS conference on User services*. Baltimore, MD, USA: ACM.
- McKean, J.R., Brogan, S.M. and Wrench, J.S. (2009), "A cross-cultural comparison of East Asian and American higher education criminal justice student learning preferences using the VARK questionnaire", *Journal of Criminal Justice Education*, Vol. 20 No. 3, pp. 272-291.
- Meehan-Andrews, T.A. (2009), "Teaching mode efficiency and learning preferences of first year nursing students", *Nurse Education Today*, Vol. 29, pp. 24-32.
- Meyer, B., Haywood, N., Sachdev, D. and Faraday, S. (2008), *"Independent learning: Literature review"*, London Department for Children, Schools and Families.
- Microsoft (2009), "Consumer online safety education", Available at: <http://www.microsoft.com/protect/default.aspx> (Accessed: 2 September 2009).
- Milne, J. (1999), "Evaluation cookbook: Questionnaires: Advantages and disadvantages", Available at: http://www.icbl.hw.ac.uk/ltidi/cookbook/info_questionnaires/index.html (Accessed: 22 July 2012).

- Mohd Noor, K.B. and Dola, K. (2012), "Leveraging training to maximizing employees performance and potential benefits", *Business and Management Review*, Vol. 1 No. 11, pp. 19-26.
- Molenda, M. (2003), "In search of the elusive ADDIE model", *Performance Improvement*, Vol. 42 No. 5, pp. 34-36.
- Murphy, R.J., Gray, S.A., Straja, S.R. and Bogert, M.C. (2004), "Student learning preferences and teaching implications", *Journal of Dental Education*, Vol. 68 No. 8, pp. 859-866.
- Mustaro, P.N. and Silveira, I.F. (2006), "Learning objects: Adaptive retrieval through learning styles", *Interdisciplinary Journal of Knowledge and Learning Objects*, Vol. 2, pp. 35-46.
- National College (2008), "*Leading personalising learning national survey: Executive summary*". Available at: <http://www.nationalcollege.org.uk/docinfo?id=31445&filename=pl-national-survey-summary.pdf> (Accessed: 1 November 2010).
- National College (2010), "About key components of personalised learning", Available at: <http://www.nationalcollege.org.uk/index/leadershiplibrary/leadingschools/personalisedlearning/key-components-of-personalised-learning-2/key-components-personalised-learning-about.htm> (Accessed: 27 October 2010).
- National Cyber Security Alliance and Symantec (2008), "*NCSA-Symantec national cyber security awareness study newsworthy analysis*". 1-3 pp.
- NCSA (2008), "Staysafe online.org", Available at: <http://staysafeonline.org/> (Accessed: 2 February 2008).
- NCSA (2010), "*2010 NCSA / Norton by Symantec online safety study*", National Cyber Security Alliance, Norton by Symantec and Zogby International 13 pp. Available at: <http://staysafeonline.mediaroom.com/download/FINAL+NCSA+Full+Online+Safety+Study+2010%5B1%5D.pdf> (Accessed: 9 July 2012).
- Neha (2013), "Flowchart", Available at: <http://www.whatsupnew.com/wp-content/uploads/flowchart.jpg> (Accessed: 19 January 2014).
- Network Dictionary. Com (2008), "Information, computer and network security", Available at: <http://www.networkdictionary.com/Information+Security%2C+network+security%2C+computer+security> (Accessed: 8 May 2008).
- NIST (2003), "*Building an information technology security awareness and training program (NIST Special Publication No. 800-50)*", National Institute of Standards and Technology. Available at: <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf> (Accessed: 5 May 2011).
- Nolting, P.D. (2002), "*Winning a math: Your guide to learning mathematics through successful study skills* ", 4th edition, Bradenton, FL: Academic Success Press.
- Novak, S. (2006), "Pharmacy students' learning styles before and after a problem-based learning experience", *American Journal of Pharmaceutical Education*, Vol. 70 No. 4, pp. 1-8.

- Okenyi, P.O. and Owens, T.J. (2007), "On the Anatomy of Human Hacking", *Information Systems Security*, Vol. 16, pp. 302-314.
- Oosterheert, I.E. and Vermunt, J.D. (2001), "Individual differences in learning to teach: relating cognition, regulation and affect", *Learning and Instruction*, Vol. 11 No. 2, pp. 133-156.
- Oxford Dictionaries (2012), "Oxford Dictionaries: The world's most trusted dictionaries", Available at: <http://oxforddictionaries.com/> (Accessed: 18 July 2012).
- Paludan, J.P. (ed.) (2006) *Personalised learning 2025*. Schooling for Tomorrow: Personalising Education. Paris: OECD.
- Park, C.C. (1997), "Learning style preferences of Asian American (Chinese, Filipino, Korean, and Vietnamese) students in secondary schools", *Equity Excellence in Education*, Vol. 30 No. 2, pp. 68-77.
- Pfheleger, C.P. (1997), "*Security in computing*", United States of America: Prentice Hall.
- Pigg, K.E., Busch, L. and Lacy, W.B. (1980), "Learning styles in Adult education: A study of county extension agents", *Adult Education Quarterly*, Vol. 30 No. 4, pp. 233-244.
- Power, R. and Forte, D. (2006), "Social engineering: attacks have evolved, but countermeasures have not", *Computer Fraud & Security*, Vol. 2006 No. 10, pp. 17-20.
- Prain, V., Cox, P., Deed, C., Dorman, J., Edwards, D., Farrelly, C., Keeffe, M., Lovejoy, V., Mow, L., Sellings, P., Waldrip, B. and Yager, Z. (2012), "Personalised learning: lessons to be learnt", *British Educational Research Journal*, pp. 1-23.
- Pratt, D.D. (1992), "Conceptions of teaching", *Adult Education Quarterly*, Vol. 42, pp. 203-220.
- Pritchard, A. (2005), "*Ways of Learning: Learning Theories and Learning Styles in the Classroom*", London: David Fulton Publishers.
- Quayle, E. and Taylor, M. (2002), "Paedophiles, pornography and the Internet: Assessment issues", *The British Journal of Social Work*, Vol. 32 No. 7, pp. 863-873.
- Rakap, S. (2010), "Impacts of learning styles and computer skills on adult students' learning online", *The Turkish Online Journal of Educational Technology*, Vol. 9 No. 2, pp. 108-115.
- Rangaswamy, N. and Cutrell, E. (2012) 'Anthropology, development and ICTs: Slums, youth and the mobile Internet in urban India'. *International Conference on Information and Communication Technologies and Development*. Atlanta, GA: 12-15 March 2012 ACM. Available at: http://research.microsoft.com/en-us/um/people/cutrell/ICTD2012-Rangaswamy_Anthropologists_and_ICTD.pdf (Accessed: 11 July 2012).
- Reischmann, J. (2004), "Andragogy. History, meaning, context, function", Available at: <http://www.uni-bamberg.de/fileadmin/andragogik/08/andragogik/andragogy/index.htm> (Accessed: 7 July 2011).
- Richardson, R. (2007), "2007 CSI computer crime and security survey", Available at: <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf> (Accessed: 22 August 2008).

- Richardson, R. (2008), "2008 CSI computer crime & security survey", Computer Security Institute. Available at: <http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf> (Accessed: 2 November 2008).
- Riding, R. and Rayner, S. (1998), "Cognitive styles and learning strategies: Understanding style differences in learning and behaviour", David Fulton Publishers.
- Rotvold, G. (2008), "How to Create a Security Culture in Your Organization", *Information Management Journal*, Vol. 42 No. 6, pp. 32-38.
- SANS (2008), "SANS infosec reading room - Home and Small Office", Available at: http://www.sans.org/reading_room/whitepapers/hsoffice/ (Accessed: 5 May 2012).
- Schlienger, T. and Teufel, S. (2003), "Analyzing information security culture: Increased trust and appropriate information security culture", *Proceedings of the 14 th International Workshop on Database and Expert Systems Applications, 2003 (DEXA'03)* Prague, Czech Republic.
- Schneier, B. (2000), "Secrets and lies", ed. Long, C., Indiana: Wiley Publishing, Inc.
- Schultz, E. (2004), "Security training and awareness--fitting a square peg in a round hole", *Computers & Security*, Vol. 23 No. 1, pp. 1-2.
- Sebba, J., Brown, N., Steward, S., Galton, M., James, M., Celentano, N. and Boddy, P. (2007), "An investigation of personalised learning approaches used by schools", Available at: <http://www.sussex.ac.uk/education/documents/rr843.pdf> (Accessed: 6 May 2010).
- Sheffield Hallam University (2011), "Dyslexia-Information for tutors", Available at: <http://www3.shu.ac.uk/hwb/placements/nursing/documents/1SHUDYSLEXIAGUIDELINES.pdf> (Accessed: 28 November 2011).
- Shuttleworth, M. (2009), "Pretest-posttest designs", Available at: <http://www.experiment-resources.com/pretest-posttest-designs.html> (Accessed: 1 May 2012).
- Sims, R.R. (1990), "Adapting training to trainee learning styles", *Journal of European Industrial Training*, Vol. 14 No. 2, pp. 17-22.
- Siponen, M.T. (2000), "A conceptual foundation for organisational information security awareness", *Information Management & Computer Security*, Vol. 8 No. 1, pp. 31-41.
- Smith, A. (2012), "17% of cell phone owners do most of their online browsing on their phone, rather than a computer or other device", Washington, D.C.: Pew Research Center's Internet & American Life Project. Available at: http://pewinternet.org/~media/Files/Reports/2012/PIP_Cell_Phone_Internet_Access.pdf (Accessed: 4 July 2012).
- Sociology.org (2012), "Sociological research skills: Name of method - Questionnaires", Available at: <http://www.sociology.org.uk/methodq.pdf> (Accessed: 21 July 2012).
- Spector, J.M. and Teja, I.d.I. (2001), "Competencies for online teaching", ERIC Clearing House on Information & Technology, Syracuse University. Available at: <http://www.ibstpi.org/downloads/online-competencies.pdf> (Accessed: 12 July 2012).

Spurge, V. and Almond, N. (2003), "Broadband technology: How developers are responding to office occupiers' needs", *Property Management*, Vol. 22 No. 2, pp. 108-126.

Spurling, P. (1995), "Promoting security awareness and commitment", *Information Management & Computer Security*, Vol. 3 No. 2, pp. 20-26.

StaySafeOnline (2009), "Are your defenses up and your instincts honed?", Available at: <http://www.staysafeonline.org/> (Accessed: 23 July 2009).

Sternberg, R.J., Grigorenko, E.L. and Zhang, L.-f. (2008), "Styles of learning and thinking matter in instruction and assessment", *Perspectives on Psychological Science*, Vol. 3 No. 6, pp. 486-506.

Sturman, L., Lewis, K., Morrison, J., Scott, E., Smith, P., Styles, B., Taggart, G. and Woodthorpe, A. (2005), "*General teaching council survey of teachers 2005*".

Swaak, M. (2009), "Effects of information usefulness, visual attractiveness, and usability on web visitors' trust and behavioral intentions", *Proceedings of the IEEE International Professional Communication Conference, 2009. IPCC 2009*, Univ. of Twente, Enschede, Netherlands.

Syed-Khuzzan, S.M. and Goulding, J.S. (2009), "Personalised learning environments (part 2): a conceptual model for construction", *Industrial & Commercial Training*, Vol. 41 No. 1, pp. 47-56.

Symantec (2007), "*Symantec Internet security threat report - Trends for January - June 2007*", Symantec Corporation. 134 pp. Available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf (Accessed: 2 July 2008).

Symantec (2008), "*Symantec Internet security threat report - Trends for July - December 2007*". Available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf (Accessed: 12 September 2008).

Symantec (2011), "*Norton Cybercrime Report 2011*", Symantec Corporation. Available at: http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/ (Accessed: 4 July 2012).

Taylor, S. and Todd, P.A. (1995), "Understanding information technology usage: A test of competing models", *Information Systems Research*, Vol. 6 No. 2, pp. 144-176.

The National Strategies (2007), "Leading on intervention: Personalisation questions and answers", Available at: <http://nationalstrategies.standards.dcsf.gov.uk/downloader/9e2a483e7a1c9191f017c6ddfe2dfc30.pdf> (Accessed: 30 March 2010).

The Trustees of Indiana University (2005), "Windows: End user security: What you don't know can hurt you: Computer security terminology", Available at: http://ittraining.iu.edu/workshops/win_security/terminology.html (Accessed: 9 May 2008).

Thomas, C.S. and Carvalho, F. (2012), "*Reaching the third billion: Arriving at affordable broadband to stimulate economic transformation in emerging markets*". Available at:

http://www3.weforum.org/docs/GITR/2012/GITR_Chapter1.6_2012.pdf (Accessed: 11 July 2012).

Thompson, M.E. and Von Solms, R. (1998), "Information security awareness: Educating your users effectively", *Information Management & Computer Security*, Vol. 6 No. 4, pp. 167-173.

Thomson, K. and van Niekerk, J. (2012), "Combating information security apathy by encouraging prosocial organisational behaviour", *Information Management & Computer Security*, Vol. 20 No. 1, pp. 39-46.

Toan-Thinh, T., Minh-Triet, T. and Anh-Duc, D. (2012), "Improvement of the More Efficient and Secure ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on ECC", *Proceedings of the Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*, pp. 698-703.

Tryfonas, T., Kiountouzis, E. and Poulymenakou, A. (2001), "Embedding security practices in contemporary information systems development approaches", *Information Management & Computer Security*, Vol. 9 No. 4, pp. 183-197.

Turn, R. (1986), "Security and privacy requirements in computing", *Proceedings of the Proceedings of 1986 ACM Fall joint computer conference*, Dallas, Texas, United States, pp. 1106-1114.

Underwood, J. and Banyard, P. (2008), "Managers', teachers' and learners' perceptions of personalised learning: evidence from Impact 2007", *Technology, Pedagogy and Education*, Vol. 17 No. 3, pp. 233 - 246.

Van Blerkom, D.L. (2006), "*College study skills: Becoming a strategic learner*", 5th edition, Boston: Thompson Higher Education.

Vincent, A. and Ross, D. (2001a), "Learning Style Awareness", *Journal of Research on Computing in Education*, Vol. 33 No. 5, pp. 1-10.

Vincent, A. and Ross, D. (2001b), "Personalise training: Determine learning style, personality types and multiple intelligence", *The Learning Organisation*, Vol. 8 No. 1, pp. 36-43.

von Solms, B. (2000), "Information Security -- The Third Wave?", *Computers & Security*, Vol. 19 No. 7, pp. 615-620.

von Solms, B. (2006), "Information Security - The Fourth Wave", *Computers & Security*, Vol. 25 No. 3, pp. 165-168.

von Solms, R. and von Solms, S.H. (2006), "Information security governance: Due care", *Computers & Security*, Vol. 25 No. 7, pp. 494-497.

Wallop, H. (2007), "Fears over Facebook identity fraud.", Available at: <http://www.telegraph.co.uk/news/uknews/1556322/Fears-over-Facebook-identity-fraud.html> (Accessed: 2 September 2009).

Watkins, C. (2010), "Learning about learning", Available at: http://www.ioe.ac.uk/about/documents/Watkins_09_Lng_about_lng.pdf (Accessed: 19 August 2010).

- Watson, J. and Hardaker, G. (2005), "Steps toward personalised learner management systems (LMS): SCORM implementation ", *Campus-Wide Information Systems*, Vol. 21, pp. 56-70.
- WebWise (2012), "The BBC guide to using the Internet.", Available at: <http://www.bbc.co.uk/webwise/> (Accessed: 1 September 2012).
- Wehrwein, E.A., Lujan, H.L. and DiCarlo, S.E. (2007), "Gender differences in learning style preferences among undergraduate physiology students", *Advances in Physiology Education*, Vol. 31, pp. 153-157.
- White, G. (2009), "Strategic, tactical, & operational management security model", *Journal of Computer Information Systems*, Vol. 49 No. 3, pp. 71-75.
- Whitman, M.E. and Mattord, H. (2005), "*Principles of information security*", Boston: Course Technology.
- Wiley, D.A. (2000) 'Learning object design and sequencing theory'. [PhD Thesis] Brigham Young University.
- Williams, P.A.H. (2008), "In a 'trusting' environment, everyone is responsible for information security", *Information Security Technical Report*, Vol. 13 No. 4, pp. 207-215.
- Wilson, M. and Hash, J. (2003) *Building an information technology security awareness and training program*. 800-50 Division, C.S. National Institute of Standards and Technology (NIST).
- Wired Safety (2012), "The world's first Internet safety and help group", Available at: <http://www.wiredsafety.org/> (Accessed: 10 May 2012).
- Wolf, M., Haworth, D. and Pietron, L. (2011), "Measuring an information security awareness program", *Review of Business Information Systems*, Vol. 15 No. 3, pp. 9-22.
- Wood, C.C. (1995), "Information security awareness raising methods", *Computer Fraud & Security Bulletin*, Vol. 1995 No. 6, pp. 13-15.
- Wood, C.C. (1997), "Policies alone do not constitute a sufficient awareness effort", *Computer Fraud & Security*, Vol. 1997 No. 12, pp. 14-19.
- Wright, M.A. and Kakalik, J.S. (2007), "*Information security: Contemporary cases*", Sudbury, Massachusetts: Jones and Bartlett Publishers.
- Yuen-Yan, C. and Wei, V.K. (2009), "Teaching for conceptual change in security awareness: A case study in higher education", *Security & Privacy, IEEE*, Vol. 7 No. 1, pp. 68-71.
- Yurcik, W. and Doss, D. (2001) 'Different approaches in the teaching of information systems security'. *Information Systems Education Conference (ISECON)*. Cincinnati, OH.

Appendix A

Faculty of Technology Ethical Approval Application Form

UNIVERSITY OF PLYMOUTH
FACULTY OF TECHNOLOGY



Faculty of Technology Research Ethics Committee (FTEC)

**Application for ethical approval of undergraduate or postgraduate
(taught) project involving human participants**

Before you complete this form please read all the notes at the back of the form

1. Title of project:

Transferability of Information Security Knowledge

2. Contact details

Name and email address of:

- Applicant: Shuhaili Talib (shuhaili.talib@plymouth.ac.uk)
- Project supervisor: 1) Dr. Nathan Clarke (N.Clarke@plymouth.ac.uk)
2) Prof. Steven Furnell (S.Furnell@plymouth.ac.uk)

Title of undergraduate or postgraduate (taught) programme:

MPhil/PhD Information Security

3. Proposed dates and duration of project

PhD Project : 1st October 2007 - 31st October 2010 (3 years)

Survey Timeline: 1st August 2008 – 1st October 2008

Duration: 3 months (For survey)

4. Aims and objectives of project

The aim of the project is to understand and assess the degree of knowledge transfer that exists between the work and home environment with respect to information security. The objectives of the project are:

- 1) To understand/assess the current level of information security awareness among staff.
- 2) To understand/assess sources of information security knowledge.
- 3) To understand/assess the current information security practices in the workplace and at home.
- 4) To identify the transferability of information security knowledge/skills from workplace to home and vice versa.
- 5) To find out what type of training approaches people prefer most.

5. Project details

An online survey will be conducted and participants will be invited through email. The potential participants are going to be identified based on the researcher's academic contacts, friends and from the word-of-mouth. Each participant will be asked to answer 44 questions (in addition to a number of optional questions depending upon their responses bringing the total number of possible questions to 83) in total. The survey will take approximately 15-20 minutes to complete and none of the questions are of a sensitive nature. Participants for this study are considered to be those who are working in any organisation who have access to the Internet and computing facilities both at work and at home. The target number of participants is in the range of 150-200.

6. Ethical protocol

(a) Informed Consent:

Respondents will be informed of the project aims at the beginning of the survey. The respondent will consent that their data will be used anonymously for the aims of the study by clicking on start the survey.

(b) Openness and Honesty:

The aim and the procedures of the research will be made clear to participants at the beginning of the survey, and there is no intention or requirement to deceive the participants.

(c) Right to Withdraw:

The participants will be informed that they have the right to withdraw at any time at the beginning of the survey. They will also have the right to withhold any data collected from them up to the point of their withdrawal. Unfortunately, given the anonymous storage of the survey results, once the survey has been submitted it will not be possible to identify and therefore delete any individual user's data.

(d) Protection From Harm or Distress:

The answers will not contain any personal information. It is recognised that the nature of the questions may cause some respondent to finish with a heightened concern about their security, and wanting to know what to do about it. As such, the researcher will be prepared to offer brief advice in this respect.

(e) Debriefing:

The purpose of the study will be explained at the beginning of the survey.

(f) Confidentiality:

The participants' identity will be protected as their names will not be mentioned anywhere. None of the results reported from the study will include information that allows identification of named individuals.

7. Declaration

By completing this form and emailing it to my project supervisor, I confirm that, to the best of my knowledge, this project conforms to the ethical principles laid down by the University of Plymouth. I also confirm that I have attached the following

- Copy of questionnaire [attached]
- Copy of opening paragraph of the questionnaire [attached]

Date of submission: 11 July 2008

Completed forms should be forwarded by email to your project supervisor who will then forward them to the Secretary (Sarah Tilley, Faculty Business Manager, sarah.tilley@plymouth.ac.uk).

Annex 1 of the University's Research Ethics Policy

Ethical principles for research involving human participants

1. Informed consent

The researcher should, where possible, inform potential participants in advance of any features of the research that might reasonably be expected to influence their willingness to take part in the study.

Where the research topic is sensitive, the ethical protocol should include verbatim instructions for the informed consent procedure and consent should be obtained in writing.

Where children are concerned, informed consent may be obtained from parents or teachers acting in loco parentis, or from the children themselves if they are of sufficient understanding. However, where the topic of research is sensitive, written informed consent should be obtained from individual parents.

2. Openness and honesty

So far as possible, researchers should be open and honest about the research, its purpose and application.

Some types of research appear to require deception in order to achieve their scientific purpose. Deception will be approved in experimental procedures only if the following conditions are met:

- a. Deception is completely unavoidable if the purpose of the research is to be achieved.
- b. The research objective has strong scientific merit.
- c. Any potential harm arising from the proposed deception can be effectively neutralised or reversed by the proposed debriefing procedures (see section 5).

Failing to inform participants of the specific purpose of the study at the outset is not normally considered to be deception, provided that adequate informed consent and debriefing procedures are proposed.

Covert observation should be resorted to only where it is impossible to use other methods to obtain essential data. Ideally, where informed consent has not been obtained prior to the research it should be obtained post hoc.

3. Right to withdraw

Where possible, participants should be informed at the outset of the study that they have the right to withdraw at any time without penalty.

In the case of children, those acting in loco parentis or the children themselves if of sufficient understanding, shall be informed of the right to withdraw from participation in the study.

4. Protection from Harm

Researchers must endeavour to protect participants from physical and psychological harm at all times during the investigation.

Note that where stressful or hazardous procedures are concerned, obtaining informed consent whilst essential, does not absolve the researcher from responsibility for protecting the participant. In such cases, the ethical protocol must specify the means by which the participant will be protected, e.g. by the availability of qualified medical assistance.

Where physical or mental harm nevertheless does result from research procedure, investigators are obliged to take action to remedy the problems created.

5. Debriefing

Researchers should, where possible, provide an account of the purpose of the study as well as its procedures. If this is not possible at the outset, then ideally it should be provided on completion of the study.

6. Confidentiality

Except with the consent of the participant, researchers are required to ensure confidentiality of the participant's identity and data throughout the conduct and reporting of the research.

Ethical protocols may need to specify procedures for how this will be achieved. For example, transcriptions of the interviews may be encoded by the secretary so that no written record of the participant's name and data exist side by side. Where records are held on computer, the Data Protection Act also applies.

7. Ethical principles of professional bodies

This set of principles is generic and not exhaustive of considerations which apply in all disciplines. Where relevant professional bodies have published their own guidelines and principles, these must be followed and the current principles interpreted and extended as necessary in this context.

Guidelines on informed consent

Potential participants must be given sufficient information to allow them to decide whether or not they wish to take part. This is the notion of 'informed consent'. This is achieved by providing a 'participant information sheet' and a consent form. The grid below sets out guidelines on who will need to see the participant information sheet, who can give consent, and how to evidence this. A participant information sheet template is provided on page 6 and a model consent form on page 7.

Survey method	Primary School	Secondary School	Sixth form	Adult
Questionnaire	<p>Consent by teacher</p> <p>Signs one form on behalf of the whole class.</p> <p>Participant information sheet to teacher only</p>	<p>Consent by teacher</p> <p>Signs one form on behalf of the whole class.</p> <p>Participant information sheet to teacher only</p>	<p>No consent form needed: consent implied by completing questionnaire.</p> <p>Information sheet to all participants – can be first part of questionnaire</p>	<p>No consent form needed: consent implied by completing questionnaire.</p> <p>Information sheet to all participants – can be first part of questionnaire</p>
Test/ worksheet/ class activities (written record only)	<p>Consent by teacher.</p> <p>Signs one form on behalf of class.</p> <p>Information sheet to teacher only: teacher or researcher to raise information sheet issues, eg right to withdraw, at start of activity</p>	<p>Consent by teacher.</p> <p>Signs one form on behalf of class.</p> <p>Information sheet to teacher only: teacher or researcher to raise information sheet issues, eg right to withdraw, at start of activity</p>	<p>Consent by participant.</p> <p>Needs to see information sheet and to sign consent form. Both can be included as the first part of the test, etc</p>	<p>Consent by participant.</p> <p>Needs to see information sheet and to sign consent form. Both can be included as the first part of the test, etc</p>
Interview, focus group etc (written record only)	<p>Consent by teacher.</p> <p>Signs one form on behalf of class.</p> <p>Information sheet to teacher only. Teacher or researcher to raise information sheet issues, eg right to withdraw, at start of activity</p>	<p>Consent by teacher.</p> <p>Signs one form on behalf of class.</p> <p>Information sheet to teacher only: teacher or researcher to raise information sheet issues, eg right to withdraw, at start of activity</p>	<p>Consent by participant.</p> <p>Researcher goes through information sheet at the start of the interview etc. Participants consent by taking part</p>	<p>Consent by participant.</p> <p>Researcher goes through information sheet at the start of the interview etc. Participants consent by taking part</p>

<p>Recording of any interview, activity etc (by video, audio, etc)</p>	<p>Consent by parent. Needs to see information sheet and sign consent form to confirm their child can take part</p>	<p>Consent by parent. Needs to see information sheet and sign consent form to confirm their child can take part</p>	<p>Consent by participant. Needs to read information sheet and sign consent form or begin by recording their consent</p>	<p>Consent by participant. Needs to read information sheet and sign consent form or begin by recording their consent</p>
---	---	---	--	--

Participant Information Sheet Template

The purpose of the participant information sheet is to provide, in lay terms, sufficient information for potential participants to make an informed choice. Thus it needs to include such information as the nature of the study; what is expected of participants; their right to withdraw; how their data / results will be collected and kept confidential. It is important that the information sheet should be written in simple, non-technical terms and be easily understood by a lay person. While it is always important to ensure that adequate information is given, the way in which the information is presented will need to be adapted to the individual study.

The information sheet should normally contain the following information:

Study title

The title should be simple and self-explanatory to a lay person.

Invitation paragraph

This should explain that the individual is being asked to take part in a research study. The following is an example of how this may be phrased:

“You are being invited to take part in a research study. Before you decide it is important for you to understand why the research is being done and what it will involve. Please take time to read the following information carefully.”

What is the purpose of the study?

The background and the aim of the study should be clearly described here. You should say how long the study will run and outline the overall design of the study.

Why have I been chosen?

You should explain how the individual was chosen to take part in the study and how many other people will be asked to participate.

Do I have to take part?

You should explain that taking part in the research is entirely voluntary. For example, you could say:

“It is up to you to decide whether or not to take part. If you do decide to take part you will be given this information sheet to keep and be asked to sign a consent form. If you decide to take part you are still free to withdraw at any time and without giving a reason.”

What will happen to me if I take part?

You should explain your methods of data collection, including what the individual will be asked to do and how much time will be involved.

What are the possible disadvantages and risks of taking part? (Where appropriate)

You should describe any disadvantages or 'costs' involved in taking part in the study, including the time involved.

What are the possible benefits of taking part?

You should outline any direct benefits for the individual and any other beneficial outcomes of the study, including furthering our understanding of the topic.

Will what I say in this study be kept confidential?

You should explain that all information collected about the individual will be kept strictly confidential and describe how confidentiality, privacy and anonymity will be ensured in the collection, storage and publication of research material.

What will happen to the results of the research study?

You should tell the individual what will happen to the results of the research. Will they be used in your dissertation or thesis? For what degree? Will they be published? How can they obtain a copy of the published research?

Who is organising the research?

You should explain that you are conducting the research as a student of the School of Engineering/ School of Mathematics and Statistics, Faculty of Technology, University of Plymouth.

Who has reviewed the study?

You may state that the research has been approved by the Faculty of Technology Research Ethics Committee.

Contact for Further Information

You should give the individual a contact point for further information. This can be your name or that of your project supervisor. You should add that if they have any concerns about the way in which the study has been conducted, they should contact the Faculty of Technology Business Manager who is secretary of the Faculty of Technology Research Ethics Committee. Current contact details are:

Sarah Tilley
Faculty of Technology Business Manager
University of Plymouth
Drake Circus
Plymouth
PL4 8AA

Phone: 01752 233311
Email: sarah.tilley@plymouth.ac.uk

Thank you

Remember to thank the individual for taking time to read the information sheet!

Date

The information sheet should be dated.

Debriefing

It is customary at the end of the study that participants are debriefed. In most cases this will involve no more than thanking the participants and asking them if they have any questions.

CONSENT FORM

FACULTY OF TECHNOLOGY

Full title of project: Transferability of Information Security Knowledge



Name of researcher: Shuhaili Talib

Please Initial Box

1. I confirm that I have read and understand the information sheet for the above study and have had the opportunity to ask questions.

2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving reason.

3. I agree to take part in the above study.

Note for researchers: Include the following statements if appropriate, or delete from your consent form:

4. I agree to the interview / focus group / consultation being audio recorded.

5. I agree to the interview / focus group / consultation being video recorded.

6. I agree to the use of anonymised quotes in publications

Name of Participant

Date

Signature

Shuhaili Talib

Name of Researcher

Date

Signature

Appendix B

The Transferability of Information Security Knowledge Survey



University of Plymouth

Transferability of Information Security Knowledge**Section A: Demographics***** Q1: Q1: Please select your gender:**Please choose *only one* of the following:

- Female
 Male

*** Q2: Q2: To what age group do you belong?**Please choose *only one* of the following:

- 16-24
 25-34
 35-44
 45-54
 55+

*** Q3: Q3: Please select your location (Country):**Please choose *only one* of the following:

- Afghanistan
 Albania
 Algeria
 Andorra
 Angola
 Antigua and Barbuda
 Argentina
 Armenia
 Australia
 Austria
 Azerbaijan
 The Bahamas
 Bahrain
 Bangladesh
 Barbados
 Belarus
 Belgium
 Belize
 Benin
 Bhutan
 Bolivia
 Bosnia and Herzegovina
 Botswana
 Brazil
 Brunei
 Bulgaria
 Burkina Faso
 Burundi
 Cambodia
 Cameroon
 Canada
 Cape Verde

- Central African Republic
- Chad
- Chile
- China
- Colombia
- Comoros
- Congo, Republic of the
- Congo, Democratic Republic of the
- Costa Rica
- Cote d'Ivoire
- Croatia
- Cuba
- Cyprus
- Czech Republic
- Denmark
- Djibouti
- Dominica
- Dominican Republic
- East Timor
- Ecuador
- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Ethiopia
- Fiji
- Finland
- France
- Gabon
- Gambia (The)
- Georgia
- Germany
- Ghana
- Greece
- Grenada
- Guatemala
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Honduras
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland (Southern)
- Israel
- Italy
- Jamaica
- Japan
- Jordan
- Kazakhstan

- Kenya
- Kiribati
- Korea, North
- Korea, South
- Kuwait
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Lesotho
- Liberia
- Libya
- Liechtenstein
- Lithuania
- Luxembourg
- Macedonia
- Madagascar
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Mauritania
- Mauritius
- Mexico
- Federated States of Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Morocco
- Mozambique
- Myanmar (Burma)
- Namibia
- Nauru
- Nepal
- Netherlands
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Norway
- Oman
- Pakistan
- Palau
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Poland
- Portugal
- Qatar
- Romania

- Russia
- Rwanda
- Saint Kitts and Nevis
- Saint Lucia
- Saint Vincent and the Grenadines
- Samoa
- San Marino
- Sao Tome and Principe
- Saudi Arabia
- Senegal
- Serbia and Montenegro
- Seychelles
- Sierra Leone
- Singapore
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- Spain
- Sri Lanka
- Sudan
- Suriname
- Swaziland
- Sweden
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- Togo
- Tonga
- Trinidad and Tobago
- Tunisia
- Turkey
- Turkmenistan
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates (UAE)
- United Kingdom
- United States
- Uruguay
- Uzbekistan
- Vanuatu
- Vatican City (Holy See)
- Venezuela
- Vietnam
- Yemen
- Zambia
- Zimbabwe

* Q4: Q4: What is your highest level of education?

<p>Please choose *only one* of the following:</p> <p><input type="checkbox"/> School</p> <p><input type="checkbox"/> College</p> <p><input type="checkbox"/> Undergraduate</p> <p><input type="checkbox"/> Postgraduate</p> <p><input type="checkbox"/> Doctorate</p> <p><input type="checkbox"/> Other <input type="text"/></p>
<p>* Q5: Q5: In what industry is your organisation?</p> <p>Please choose *only one* of the following:</p> <p><input type="checkbox"/> Accounting/Finance</p> <p><input type="checkbox"/> Advertising/Public Relations</p> <p><input type="checkbox"/> Art/Entertainment/Publishing</p> <p><input type="checkbox"/> Banking/Mortgage</p> <p><input type="checkbox"/> Clerical/Administrative</p> <p><input type="checkbox"/> Construction/Facilities</p> <p><input type="checkbox"/> Customer Service</p> <p><input type="checkbox"/> Education/Training</p> <p><input type="checkbox"/> Engineering/Architecture</p> <p><input type="checkbox"/> Government</p> <p><input type="checkbox"/> Healthcare</p> <p><input type="checkbox"/> Hospitality/Travel</p> <p><input type="checkbox"/> Human Resources</p> <p><input type="checkbox"/> Insurance</p> <p><input type="checkbox"/> Internet/New Media</p> <p><input type="checkbox"/> Law Enforcement/Security</p> <p><input type="checkbox"/> Legal</p> <p><input type="checkbox"/> Management Consulting</p> <p><input type="checkbox"/> Manufacturing/Operations</p> <p><input type="checkbox"/> Marketing</p> <p><input type="checkbox"/> Military</p> <p><input type="checkbox"/> Non-profit</p> <p><input type="checkbox"/> Pharmaceutical/Biotech</p> <p><input type="checkbox"/> Real Estate</p> <p><input type="checkbox"/> Restaurant/Food Service</p> <p><input type="checkbox"/> Retail</p> <p><input type="checkbox"/> Sales</p> <p><input type="checkbox"/> Technology</p> <p><input type="checkbox"/> Telecommunications</p> <p><input type="checkbox"/> Transportation/Logistics</p> <p><input type="checkbox"/> Other</p>
<p>[Only answer this question if you answered 'Other' to question 'Q5']</p> <p>* Q5A: Q5A: If Other, please specify:</p> <p>Please write your answer here:</p> <p><input type="text"/></p>
<p>* Q6: Q6: What is the size of your organisation?</p> <p>Please choose *only one* of the following:</p> <p><input type="checkbox"/> 1 – 49 employees</p> <p><input type="checkbox"/> 50 – 99 employees</p> <p><input type="checkbox"/> 100 – 250 employees</p> <p><input type="checkbox"/> 251 - 499 employees</p> <p><input type="checkbox"/> 500 – 999 employees</p> <p><input type="checkbox"/> 1000+ employees</p>

* Q7: Q7: What is your primary role within the organisation?

Please choose **only one** of the following:

- Owner/Proprietor
 Senior Management (e.g. CEO, CFO, CIO)
 Management
 Team Leader/Supervisor
 Employee
 Other [

Section B: Information Security Awareness

* Q8: Q8: How do you rate your information security awareness level?

Please choose **only one** of the following:

- Very low
 Low
 Average
 High
 Very high
 Unsure

* Q9: Q9: How would you rate your Internet / Computing skills?

Please choose **only one** of the following:

- Beginner
 Intermediate
 Advanced
 Expert / Professional

* Q10: Q10: Who is/are responsible for information security tasks?

Please choose **all** that apply:

- Individual user
 Information security officer
 Internet Service Provider (ISP)
 System administrator
 I do not know

* Q11: Q11: Following is a list of terms relating to Information Security. For each one, please indicate whether: 1) You understand it 2) You have heard of it but are not sure what it means, 3) You never heard of it

Please choose the appropriate response for each item:

	You understand it	You have heard of it but are not sure what it means	You never heard of it
Virus/Worm	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Trojan horse	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spam	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Social engineering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phishing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Pharming	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Identity theft	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Key loggers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phlopping	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Botnets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zombies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Denial of service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Packet sniffer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Whooping	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hacker	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Zero day attacks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cracker	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Section C: Practises at Workplace
 Please answer the following questions with regards to your practise at workplace

* Q12: Q12: Does your organisation have an information security awareness program or provide related training?

Please choose *only one* of the following:

Yes
 No
 I do not know

[Only answer this question if you answered 'Yes' to question 'Q12']

* Q13: Q13: How often do you undertake information security awareness training? (Including attending workshops, seminars and self-learning through reading books/online materials)

Please choose *only one* of the following:

Never
 Once
 Daily
 Weekly
 Monthly
 Quarterly
 Half-yearly
 Yearly
 Other:

[Only answer this question if you answered 'Yes' to question 'Q12']

* Q14: Q14: Where did you receive your training?

Please choose *all* that apply:

In-house training by security experts in your organisation
 In-house training by inviting outside security experts
 Outside the organisation
 Self-reading (books/manuals)
 Online training
 Other:

[Only answer this question if you answered 'Yes' to question 'Q12']

* Q15: Q15: Which of the following security topics have been taught in your information security awareness training?

Please choose the appropriate response for each item:

	Yes	No
Security policy of the organisation	<input type="checkbox"/>	<input type="checkbox"/>
Security and risk management (e.g. reporting incidents)	<input type="checkbox"/>	<input type="checkbox"/>
Access control systems (e.g. passwords, access rights)	<input type="checkbox"/>	<input type="checkbox"/>
Network security (e.g. Internet, web)	<input type="checkbox"/>	<input type="checkbox"/>
Secure communication (e.g. file encryption)	<input type="checkbox"/>	<input type="checkbox"/>
Legal issues (e.g. copyright, intellectual properties)	<input type="checkbox"/>	<input type="checkbox"/>
Impact of security breaches on the organisation	<input type="checkbox"/>	<input type="checkbox"/>
Physical and environmental security issues	<input type="checkbox"/>	<input type="checkbox"/>

[Only answer this question if you answered 'Yes' to question 'Q12']

* Q16: Q16: Please select the type of learning method(s) that you have experienced in your previous information security awareness training?

Please choose *all* that apply:

- Cartoons
- Presentation
- Web based awareness course
- Handbooks
- Email security alerts
- Video
- Posters and screen savers
- Trinkets and gifts
- Regular bulletins
- Inspection and Audits
- Informal meetings
- Quizzes
- Information security awareness days/campaign
- Information security games

Other: _____

* Q17: Q17: What is/are the source(s) of your information security knowledge at your workplace?

Please choose *all* that apply:

- Academics journals
- Books
- Daily newspaper
- Google, Yahoo/ other search engines
- Government or professional reports
- Hearsay
- Information discussions with colleagues, professional contacts
- Interview
- Magazines
- Organisation's policy
- Pamphlets/brochures
- Posters
- Presentation
- Professional activities: conferences, meetings, briefings, etc
- Radio
- Research articles
- Television news
- Websites
- From what I learnt at home (e.g. family members, friends)

Other: _____

Q18: Q18: Please rank ONLY three (3) of the most useful sources of your information security knowledge at workplace. (Most useful <- 1 2 3 -> Least useful)

Please number each box in order of preference from 1 to 20

- Academic journals
- Books
- Daily newspaper
- Google, Yahoo / other search engines
- Government or professional reports
- Hearsay
- Information discussions with colleagues, professional contacts
- Interview
- Magazines
- Organisation's policy
- Pamphlets/brochures

Posters
 Presentation
 Professional activities: conferences, meetings, briefings, etc
 Radio
 Research articles
 Television news
 Websites
 From what I learnt at home (e.g. family members, friends)
 Other

* Q19: Q19: How often do you prefer to have information security training?

Please choose *only one* of the following:

- I am not interested
 Daily
 Weekly
 Fortnightly
 Monthly
 Quarterly
 Half-yearly
 Yearly
 On-demand/upon request
 Other [

* Q20: Q20: To what extent do the following statements are apply to you?

When using computer systems in my workplace....

Please choose the appropriate response for each item:

	Always	Sometimes	Never	Not Applicable
I log off my computer whenever I leave a computer system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I backup my data on disks or CDs regularly	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I check that antivirus software is enabled and updated	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I use the organisation's firewall protection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
my passwords consists of at least 8 characters and uses the combination of letters (a-z), symbols (!@#%&) and numbers (0-9)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I keep my password a secret and only I know it	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I change my password regularly	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I scan with antivirus any external disk/thumb drive/USB drive when first plugging it into the computer system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I report security incidents to the IT helpdesk as soon as possible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I do download or install unauthorised copies of software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I do open and execute an executable file (.exe file) from an email attachment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I do click on hyperlinks in unsolicited/spam email messages and unknown websites	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I look for "https://" or the "little gold padlock" before I make financial transactions online	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I allow a web browser (e.g. Internet Explorer (IE)/Mozilla Firefox) to save my user id(s) and passwords for faster access in the future	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I protect confidential files with passwords	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- | | | | | |
|--|--------------------------|--------------------------|--------------------------|--------------------------|
| I read the privacy statement before I proceed with an action (such as registering with a website, installing an application or financial/online banking transaction) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| I ensure nobody is looking at my keyboard each time I key in my password | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Section D: Practices at Home

Note: You might find some questions in this section are similar to the previous part. Please answer the following questions, however, with regards to your practise at home.

* Q21*: Q21: What is/are the source(s) of your information security knowledge at home?

Please choose *all* that apply:

- Academic journals
- Books
- Daily newspaper
- Google, Yahoo/other search engines
- Government or professional reports
- Hearsay
- Information discussions with colleagues, professional contacts
- Interview
- Magazines
- Organisation's policy
- Pamphlets/brochures
- Posters
- Presentation
- Professional activities: conferences, meetings, briefings, etc
- Radio
- Research articles
- Television news
- Websites
- From what I learnt at my workplace

Other:

Q22*: Q22: Please rank ONLY three (3) of the most useful sources of your information security knowledge at home. (Most useful <-1 2 3--> Least useful)

Please number each box in order of preference from 1 to 20

- Academic journals
- Books
- Daily newspaper
- Google, Yahoo/other search engines
- Government or professional reports
- Hearsay
- Information discussions with colleagues, professional contacts
- Interview
- Magazines
- Organisation's policy
- Pamphlets/brochures
- Posters
- Presentations
- Professional activities: conferences, meetings, briefings, etc
- Radio
- Research articles
- Television news
- Websites
- From what I learnt at my workplace

Other			
* Q23*: How frequently do you read articles or news about information security at home?			
<u>Please choose *only one* of the following:</u>			
<input type="checkbox"/> Never			
<input type="checkbox"/> Daily			
<input type="checkbox"/> Weekly			
<input type="checkbox"/> Monthly			
* Q24*: Q24: What is your opinion about giving your personal data on the web?			
<u>Please choose *only one* of the following:</u>			
<input type="checkbox"/> Absolutely secure			
<input type="checkbox"/> Secure with terms and conditions given by the website			
<input type="checkbox"/> Insecure even with the terms and conditions given by the website			
<input type="checkbox"/> Absolutely insecure			
<input type="checkbox"/> Other <input type="text"/>			
* Q25*: Q25: Do you *backup the data on your personal computer (PC) periodically?			
<u>Please choose *only one* of the following:</u>			
<input type="checkbox"/> Yes			
<input type="checkbox"/> No			
* Q26*: Q26: Do you use social networking websites like Facebook, Bebo, WAYN, or Friendster?			
<u>Please choose *only one* of the following:</u>			
<input type="checkbox"/> Yes			
<input type="checkbox"/> No			
<input type="checkbox"/> I do not know what it is			
[Only answer this question if you answered 'Yes' to question 'Q26*']			
* Q26A*: Q26A: What personal information have you made visible to others in your social networking websites?			
<u>Please choose *all* that apply:</u>			
<input type="checkbox"/> Real name			
<input type="checkbox"/> Email			
<input type="checkbox"/> Real date of birth			
<input type="checkbox"/> Full address			
<input type="checkbox"/> Phone number			
<input type="checkbox"/> Personal blog			
<input type="checkbox"/> Special occasions (e.g. birthday party, holiday, anniversary)			
<input type="checkbox"/> Photographs of yourself			
<input type="checkbox"/> Photographs of your family members			
<input type="checkbox"/> Photographs of your friends			
<input type="checkbox"/> Photographs of your office			
<input type="checkbox"/> Photographs of your house			
<input type="checkbox"/> None of the above			
Other: <input type="text"/>			
* Q27*: Q27: What kind of security applications/controls you are using at home?			
<u>Please choose the appropriate response for each item:</u>			
	Yes	No	I do not know
Antivirus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Firewall	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Anti-phishing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Anti-spyware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Intrusion Detection Systems (IDS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Spam filter <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>				
* Q28*: Q28: To what extent do the following statements apply to you?				
When using computer systems in my house.....				
<u>Please choose the appropriate response for each item:</u>				
	Always	Sometimes	Never	Not Applicable
I log off my computer whenever I leave a computer system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I backup my data on disks or CDs regularly	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I check that antivirus software is enabled and updated	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
my passwords consist of at least 8 characters and uses the combination of letters (a-z), symbols (!@~\$%) and numbers (0-9)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I keep my password a secret and only I know it	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I change my password regularly	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I shred confidential documents before throwing them into the bin	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I scan with antivirus any external disk/thumb drive/USB drive when first plugging it into the computer system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I report security incidents to the appropriate parties (e.g. Internet Service Provider (ISP), Computer Emergency Response Team (CERT)) as soon as possible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I do download or install unauthorised copies of software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I do open and execute an executable file (.exe file) from an email attachment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I do click on hyperlinks in unsolicited/spam email messages and unknown websites	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I look for "https://" or the "little gold padlock" before I make financial transactions online	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I allow a web browser (e.g. Internet Explorer (IE)/Mozilla Firefox) to save my user id(s) and passwords for faster access in the future	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I protect confidential files with password	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I change the default password for my router	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I use encryption key to protect my wireless connection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I read the privacy statement before I proceed with an action (such as registering with a website, installing an application or financial/online banking transaction)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I ensure nobody is looking at my keyboard each time I key in my password	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Q29*: Q29: If you have any suggestions for improving information security awareness training, please write in the space provided:				
<u>Please write your answer here:</u>				
Submit Your Survey.				
Thank you for completing this survey. Please fax your completed survey to: +44 (0) 1752 586300.				

Appendix C

The First Version of Survey Questions

Transferability of Information Security Knowledge Survey



MPhil/PhD Information Security

University of Plymouth

April 2008

Information security knowledge is an area of knowledge concerns with protection of information from unauthorized access, modifications or destructions. This questionnaire seeks to investigate the transferability of information security knowledge between workplace and home and to determine reasons why people would like to transfer such knowledge and practise it at home.

The study is being conducted as part of a PhD research project at the University of Plymouth, and the findings will contribute towards the investigation of the transferability of information security knowledge and skills from workplace to home. The outputs from this study are likely to include academic reports, and publication(s) in academic conferences and/or journals.

Appropriate participants for this study are considered to be those who are working in any organisation and having computer/laptop at home.

As much as we value your responses to this study, it is important to note that participation is voluntary, and respondents have the right to withdraw at any time. The questionnaire will require about 10-15 minutes to complete. Your responses will be treated as confidential and at all times data will be presented in such a way that your identity cannot be connected with specific published data. Outputs from the study will be available to participants via the researcher, Shuhaili Talib:

Thank you very much for your time.

Shuhaili Talib, Information Security & Network Research Group, University of Plymouth, Drake Circus, PL4 8AA, Plymouth, UK.
Email: shuhaili.talib@plymouth.ac.uk

For more information please visit: [our website](#)

The questionnaire is organized as follows:

- Section A: Demographics
- Section B: Information Security Knowledge Background
- Section C: Information Security Practises at Workplace
- Section D: Information Security Practises at Home
- Section E: Preferable Information Security Learning Method

Section A: Demographics

Q1: Please select your gender:

- a) Male
- b) Female

Q2: Please select the range of years that reflects your current age:

- a) 15 – 24
- b) 25 – 34
- c) 35 – 49
- d) 50 – 59
- e) 60+

Q3: Please select your location (Country):

-lists of countries will be made available by the online survey software.

Q4: What is your highest level of education?

- a) School
- b) College
- c) Undergraduate
- d) Postgraduate
- e) Doctorate
- f) Other (Specify)_____

Q5: In what industry is your organisation?

- a) Accounting/Finance
- b) Advertising/Public Relations
- c) Art//Entertainment/Publishing
- d) Banking/Mortgage
- e) Clerical/Administrative
- f) Construction/Facilities
- g) Customer Service
- h) Education/Training
- i) Engineering/Architecture
- j) Government
- k) Healthcare
- l) Hospitality/Travel
- m) Human Resources
- n) Insurance
- o) Internet/New Media
- p) Law Enforcement/Security
- q) Legal
- r) Management Consulting
- s) Manufacturing/Operations
- t) Marketing
- u) Military
- v) Non-profit
- w) Pharmaceutical/Biotech
- x) Real Estate

- y) Restaurant/Food Service
- z) Retail
- aa) Sales
- bb) Technology
- cc) Telecommunications
- dd) Transportation/Logistics
- ee) Other (Specify) _____

Q6: What is the size of your organisation?

Choose only one of the following

- a) 1 – 49 employees
- b) 50 – 99 employees
- c) 100 – 499 employees
- d) 500 – 999 employees
- e) 1000+ employees
- f) Other (Specify) _____

Q7: What is your role within the organisation?

- a) Administrative / Clerical / Secretarial
- b) Management
- c) Educator
- d) Sales / Marketing / Customer Services
- e) Technical
- f) System Administrator
- g) Information Security Officer
- h) Security Officer
- i) IT staff
- j) Other (Specify) _____

Q8: How would you rate your Internet / Computing skills?

- a) Beginner
- b) Intermediate
- c) Advanced
- d) Expert / Professional

Section B: Information Security Knowledge Background

Q9: Following is a list of terms relating to Information Security. For each one, please indicate whether: 1) *You understand it* 2) *You have heard it but are not sure what it means*, 3) *You never heard of it*

- a) Virus / Worm
- b) Spam
- c) Social engineering / Phishing
- d) Identity theft
- e) Denial of service
- f) Packet sniffer
- g) Hackers

Q10: Does your organisation have an information security awareness program or provide related training?

- a) Yes
- b) No
- c) I do not know

If YES, go to Q11 & Q12 if NO go to Q13.

Q11: How often do you attend security awareness programme or training?

- a) Never
- b) Daily
- c) Weekly
- d) Fortnightly
- e) Monthly
- f) Quarterly
- g) Half-yearly
- h) Yearly
- i) Other (please write in) _____

If NEVER, go to Q13.

Q12: Which of the following security topics have been taught in your information security awareness training? (Check or complete all relevant boxes)

- a) Security policy of the organisation
- b) Security and risk management (e.g. reporting incidents)
- c) Access control systems (passwords, access rights)
- d) Network security (Internet, web)
- e) Data protection/Cryptography (Protecting email messages)
- f) Legal issues (Copyright, Intellectual properties)
- g) Impact of security breaches on the organisation
- h) Physical and environmental security issues

Q13: What is/are the source(s) of your information security knowledge? (Check or complete all relevant boxes)

- a) TV news
- b) Radio
- c) Local daily newspaper
- d) Google, Yahoo/ other search engines
- e) Websites
- f) Academic journals
- g) Magazines
- h) Books
- i) Pamphlets/brochures
- j) Posters
- k) Hearsay
- l) Interview
- m) Presentation
- n) Research articles
- o) Government or professional reports
- p) Professional activities: conferences, meetings, briefings, etc
- q) Information discussions with colleagues, professional contacts
- r) Organisation's policy
- s) Other (Please write in) _____

Section C: Information Security Practises at Workplace

Q14: To what extent do the following statements are apply to you (Each statement requires a response) (*Always, Sometimes, Never*)

When using computer systems in **my workplace**

- 1) I log off my computer whenever I leave a computer systems
- 2) I backup my data on disks or CDs
- 3) I check that antivirus software is enabled and updated
- 4) I use the organisation's firewall protection
- 5) my password consists of at least 8 characters
- 6) my password uses the combination of letters (a-z), symbols (!@#\$\$%) and numbers (0-9)
- 7) my password does not use dictionary words
- 8) my password does not use personal data (names, birth date)
- 9) I write down my password in order to remember it
- 10) I do not share my password with anyone
- 11) I change my password regularly
- 12) I shred confidential documents before throwing them into the bin
- 13) I scan any external disk/thumb drive before plugging it into computer systems.
- 14) I report security incidents to the IT helpdesk as soon as possible
- 15) I do not download or install unauthorised copies of software
- 16) I do not open and execute an executable file (.exe file) from an email attachment
- 17) I do not click on hyperlinks in unsolicited/spam email messages and unknown websites
- 18) I look for "https:///" before I make financial transactions online
- 19) I allow a web browser (e.g. Internet Explorer(IE)/Mozilla Firefox) to save my user id(s) and passwords for faster access in the future
- 20) I protect confidential files with passwords

Section D: Information Security Practises at Home

Q15: To what extent do the following statements are apply to you (Each statement requires a response) (*Always, Sometimes, Never*)

When using computer systems in **my house**

- 1) I log off my computer whenever I leave a computer systems
- 2) I backup my data on disks or CDs
- 3) I check that antivirus software is enabled and updated
- 4) I use personal firewall to protect my computer
- 5) my password consists of at least 8 characters
- 6) my password uses the combination of letters (a-z), symbols (!@#%) and numbers (0-9)
- 7) my password does not use dictionary words
- 8) my password does not use personal data (names, birth date)
- 9) I write down my password in order to remember it
- 10) I do not share my password with anyone
- 11) I change my password regularly
- 12) I shred confidential documents before throwing them into the bin
- 13) I scan any external disk/thumb drive before plugging it into computer systems.
- 14) I report security incidents to the Computer Emergency Response Team (CERT) as soon as possible
- 15) I do not download or install unauthorised copies of software
- 16) I do not open and execute an executable file (.exe file) from an email attachment
- 17) I do not click on hyperlinks in unsolicited/spam email messages and unknown websites
- 18) I look for "https://" before I make financial transactions online
- 19) I allow a web browser (e.g. Internet Explorer(IE), Mozilla Firefox) to save my user id(s) and passwords for faster access in the future
- 20) I protect confidential files with passwords

Q16: Do you use **strong password* whenever you are creating password for your personal account? (e.g. personal email account, blogs or Amazon or eBay account)

- a) Always
- b) Sometimes
- c) Never

If you answer **Always**, please state why:

- a) All password should be strong regardless of system/application
- b) I feel secure when I'm using a strong password
- c) Other (Specify) _____

If you answer **Sometimes**, please state why:

- a) Only for system/application that involves with financial transactions
- b) Only when the system asked me to use strong password
- c) Other (Specify) _____

If you answer **Never**, please state why:

- a) I have no idea about strong password
- b) I do not have any password
- c) Other (Specify) _____

**Strong password is a password that contains numbers, letters and special characters (i.e. !*&^%) and do not include personal information such as name or birth date.*

Q17: Do you install firewall and antivirus at home?

- a) Yes (please state reason) _____
- b) Antivirus only (please state reason) _____
- c) Firewall only (please state reason) _____
- d) No (please state reason) _____

Q18: What is your opinion about giving your personal data on the web?

Write your answer here: _____

Q19: Do you do ****backups** for your PC from time to time?

- a) Yes (please state reason) _____
- b) No (please state reason) _____

***Backups is a process of making copies of your data and store them in CDs/external disks/USB drives.*

Q20: How often do you read articles or news about information security?

- a) Daily
- b) Fortnightly
- c) Weekly
- d) Monthly
- e) Whenever I come across the related articles.
- f) Never

Q21: Do you use social networking websites like Facebook, Beebo, WAYN, or Friendster?

- a) Yes
- b) No

If YES, go to Q22 if NO go to Q23.

Q22: Please tick the below personal information that you made visible to others in your social networking websites. (You may check more than one)

- a) Real name
- b) Email
- c) Real date of birth
- d) Full address
- e) Phone number

Q23: What did you do with your previous bank statement and ATM receipts?

- a) Keep it in a folder/file
- b) Throw them in the bin without shredding them
- c) Put them in recycle bin
- d) Shred them and throw them in the bin

Please state *why* do you answer that way.

Write your answer here: _____

Section E: Preferable Information Security Learning Method

Q24: If you were offered Information Security training, which one would you prefer? *(Please rate Good, Adequate, Poor)*

- a) Presentation and/or face to face training *(Conducting a presentation or discussion about information security issues is given to a specific group/individuals throughout the company)*
- b) Web based awareness course *(Taking an online course or tutorial about information security related issues)*
- c) Handbooks *(Providing security related handbooks: could be in hardcopy, given away to all employees, or electronic version posted on the web)*
- d) Video *(Showing videos about risks and good practices)*
- e) Email security alerts *(Posting the latest news about specific security issues: for example the information about the latest viruses and worms)*
- f) Posters and screen savers
- g) Trinkets and gifts *(Offering items imprinted with security reminders; for example, mugs, mouse pads, notepads and pens)*
- h) Regular bulletins *(Providing newsletters and magazines either electronics or paper form which contains articles on information security related issues)*
- i) Inspection and Audits *(by manager and /or security staff)*
- j) Informal meetings *(such as tea/coffee breaks to talk about information security)*
- k) Quizzes *(Having information security quizzes online)*
- l) Having Information Security Awareness days/campaigns
- m) Information Security games *(Having an information security games that enable to increase staff awareness)*

If your answer is 'Poor', please state reasons. (Is it possible for the software to come out with option why every time people answering 'Poor'?)

----- End of questionnaire -----

Appendix D

The Survey Results

Survey Results

Total respondents: 333

Section A: Demographics

Q1: Please select your gender:

Male: 184

Female: 149

Q2: To what age group do you belong?

16 – 24: 32

25 – 34: 183

35 – 44: 76

45 – 54: 31

55 and above: 11

Q3: Please select your location (Country):

Malaysia: 161

United Kingdom: 118

United States: 7

Australia: 6

Pakistan: 6

Turkey: 1

Indonesia: 4

Greece: 1

New Zealand: 3

Spain: 1

Uruguay: 1

Italy: 3

Sweden: 1

Netherlands: 3

Austria: 2

Sri Lanka: 1

Libya: 1

Norway: 3

Saudi Arabia: 3

Qatar: 2

Germany: 1

France: 1

India: 2

Malta: 1

Q4: What is your highest level of education?

School: 3

College: 22

Undergraduate: 117

Postgraduate: 153

Doctorate: 34

Other: 4:

1- Professional

2- HNC and Cert Ed

3- PQ Accountant

4- Open University

Q5: In what industry is your organisation?

Accounting/Finance: 3

Advertising/Public Relations: 1

Art/Entertainment/Publishing: 4

Banking/Mortgage: 1

Clerical/Administrative: 2

Construction/Facilities: 5

Customer Service: 2

Education/Training: 158

Engineering/Architecture: 15

Government: 25

Healthcare: 7

Hospitality/Travel: 1

Human Resources: 0

Insurance: 1

Internet/Media: 5

Law Enforcement/Security: 3

Legal: 0

Management Consulting: 2

Manufacturing/Operations: 8

Marketing: 1

Military: 1

Non-Profit: 1

Pharmaceutical/Biotech: 3

Real Estate: 1

Restaurant/Food Service: 0

Retail: 0

Sales: 0

Technology: 45

Telecommunications: 21

Transportation/Logistics: 1

Other: 16

Other's detail(s)	No. of respondents
Computer (hardware and software)	1
Computer security	1
Forest and energy	1
Information technology	2
Government company	1
IT consultant	1
ICT	1
Oil and gas	3
Research	1
Defence contracting	1

Consultant	1
Security	1
Government IT consultant	1

Q6: What is the size of your organisation?

1 – 49 employees: 40
 50 – 99 employees: 18
 100 – 250 employees: 33
 251 – 499 employees: 22
 500 – 999 employees: 34
 1000 + employees: 186

Q7: What is your primary role within the organisation?

Owner/Proprietor: 9
 Senior Management: 4
 Management: 52
 Team Leader/Supervisor: 49
 Employee: 199
 Student: 16
 Other: 4

Section B: Information Security Awareness

Q8: How do you rate your information security awareness level?

Very low: 10
 Low: 23
 Average: 134
 High: 113
 Very High: 51
 Unsure: 2

Q9: How would you rate your Internet/computer skills?

Beginner: 5
 Intermediate: 114
 Advanced: 146
 Expert/Professional: 68

Q10: Who is/are responsible for information security tasks?

Individual user: 198
 Information security officer: 147
 Internet service providers: 111
 System administrator: 232
 I do not know: 15

Q11: Following is a list of terms relating to Information Security. For each one, please indicate whether: 1) You understand it 2) You have heard of it but are not sure what it means 3) You never heard of it

Information Security Terms	You understand it	You have heard of it but are not sure it what it means	You never heard of it
Virus/Worm	308	25	0
Trojan horse	266	56	11
Spam	299	33	1
Social engineering	145	107	81
Phishing	233	67	33
Pharming	80	114	139
Identity theft	269	37	27
Key loggers	189	71	73
Phlopping	22	84	227
Botnets	111	78	144
Zombies	111	94	128
Denial of service	188	66	79
Packet sniffer	156	55	122
Whooping	34	103	196
Hacker	318	13	2
Zero day attacks	98	89	146
Cracker	186	68	79

Section C: Practises at Workplace

Q12: Does your organisation have an information security awareness program or provide related training?

Yes: 121

No: 109

I do not know: 103

Q13: How often do you undertake information security awareness training? (Including attending workshops, seminars and self-learning through reading books/online materials)

Never: 8

Once: 16

Daily: 9

Weekly: 6

Monthly: 21

Quarterly: 19

Half-yearly: 15

Yearly: 22

Other: 10

Other's detail(s)	No. of respondents
When a need arise	3
Whenever the information was passed on to me	1
When you ask for it although access restricted and locked down and rules are clear and must be signed off before access granted	1
Depends	1
Rarely	1
Free time or attending course	1
I train it and design the programme	1
Other (detail was not given)	1

Q14: Where did you receive your training?

In-house training by security experts in your organisation: 68

In-house training by inviting outside security experts: 38

Outside the organisation: 40

Self-reading (books/manuals): 71

Online training: 37

Other: 3

Other's detail(s)	No. of respondents
Master's course	1
Bulletin/newsletter/email	1
Appointed security experts department	1

Q15: Which of the following security topics have been taught in your information security awareness training?

Security policy of the organisation: 113

Security and risk management: 106

Access control systems: 111

Network security: 112

Secure communication: 85

Legal issues: 92

Impact of security breaches on the organisation: 98

Physical and environmental security issues: 97

Q16: Please select the type of learning method(s) that you have experienced in your previous information security awareness training?

Cartoons: 28

Presentation: 96

Web-based awareness course: 60
 Handbooks: 61
 Email security alerts: 81
 Video: 44
 Posters and screen savers: 34
 Trinkets and gifts: 11
 Regular bulletins: 36
 Inspection and audits: 49
 Informal meetings: 39
 Quizzes: 24
 Information security awareness days/campaign: 48
 Information security games: 13
 Other: 2

Other's detail(s)	No. of respondents
--------------------------	---------------------------

Self learn enthusiast	1
Experiment, web browse	1

Q17: What is/are the source(s) of your information security knowledge at your workplace?

Academic journals: 92
 Books: 117
 Daily newspaper: 91
 Google, Yahoo/other search engines: 192
 Government or professional reports: 61
 Hearsay: 78
 Information discussions with colleagues, professional contacts: 190
 Interview: 11
 Magazines: 115
 Organisation's policy: 156
 Pamphlets/brochures: 65
 Posters: 51
 Presentation: 90
 Professional activities (conferences, meetings, briefings, etc): 103
 Radio: 22
 Research articles: 80
 Television news: 43
 Websites: 197
 From what I learnt at home (e.g. family members, friends): 97
 *(Websites and Search engines) = 250
 Other: 13

Other's detail(s)	No. of respondents
--------------------------	---------------------------

Experience	1
Emails update from IT group	1
Notification from IT support	1
Technical podcasts	1
News letters	1

Email alerts	1
Start up screen	1
Ittutor (Online forum)	1
Email from system administrator	1
Am seeking to do a masters in the same, so have been doing some research on my own	1
System admin	1
Email subscriptions	1
I do not know	1

*For the purpose of determining the top three rank of the sources and to avoid redundancy, Websites and Googles, Yahoo or other search engines have been combined.

Q18: Please rank only three (3) of the most useful sources of your information security knowledge at workplace. (Most useful ← 1 2 3 → Least useful)

Sources of knowledge	Rank 1	Rank 2	Rank 3
Academic journals	29	11	6
Books	9	17	13
Daily newspaper	11	7	14
Websites and Search engines	102	83	69
Government or professional reports	5	6	8
Hearsay	10	7	14
Information discussions with colleagues, professional contacts	43	54	40
Interview	0	3	1
Magazines	11	6	18
Organisation's policy	59	34	18
Pamphlets/brochures	3	5	12
Posters	2	9	4
Presentation	8	11	15
Professional activities (conferences, meetings, briefings, etc)	13	31	35

Radio	0	1	5
Research articles	5	13	18
Television news	1	2	7
From what I learnt at home (e.g. family members, friends)	13	20	13
Other	1	1	8

Q19: How often do you prefer to have information security training?

I am not interested: 17

Daily: 4

Weekly: 14

Fortnightly: 7

Monthly: 49

Quarterly: 62

Half-yearly: 41

Yearly: 40

On-demand/upon request: 98

Other: 1

Q20: To what extent do the following statements apply to you? When using computer systems in my workplace....

Security Practices	Always	Sometimes	Never	Not applicable
I log off my computer whenever I leave a computer system	212	99	20	2
I backup my data on disks or CDs regularly	116	164	42	11
I check that antivirus software is enabled and updated	209	82	28	14
I use the organisation's firewall protection	265	40	16	12
My passwords consists of at least 8 characters and uses the combination of letters (a-z), symbols (!@#\$\$%) and numbers (0-9)	228	81	24	0
I keep my password a secret and only I know it	279	50	4	0
I change my password regularly	80	163	90	0

I scan with antivirus any external disk/thumb drive/USB drive when first plugging it into the computer system	129	135	58	11
I report security incidents to the IT helpdesk as soon as possible	170	97	45	21
I do download or install unauthorised copies of software	45	145	132	11
I do open and execute an executable file (.exe file) from an email attachment	32	117	176	8
I do click on hyperlinks in unsolicited/spam email messages and unknown websites	21	67	239	6
I look for "https://" or the "little gold padlock" before I make financial transactions online	208	64	37	24
I allow a web browser (e.g. Internet Explorer (IE)/Mozilla Firefox) to save my user id(s) and passwords for faster access in the future	58	131	142	2
I protect confidential files with passwords	108	141	76	8
I read the privacy statement before I proceed with an action (such as registering with a website, installing an application or financial/online banking transaction)	90	179	62	2
I ensure nobody is looking at my keyboard each time I key in my password	187	105	38	3

Section D: Practises at Home

Q21: What is/are the source(s) of your information security knowledge at home?

Academic journals: 57

Books: 94

Daily newspaper: 121

Google, Yahoo/other search engines: 209

Government or professional reports: 23

Hearsay: 67
 Information discussions with colleagues, professional contacts: 109
 Interview: 10
 Magazines: 120
 Organisation's policy: 19
 Pamphlets/brochures: 33
 Posters: 14
 Presentation: 21
 Professional activities (conferences, meetings, briefings, etc): 35
 Radio: 46
 Research articles: 42
 Television news: 84
 Websites: 192
 From what I learnt at my workplace: 124
 ** (Websites and Search engines) = 267
 Other: 7

Other's detail(s)	No. of respondents
Friends	1
Podcasts	1
News letters	1
From online guides / IT services guides	1
Personal training course ie. ECDL	1
My dad	1
Ittutor (Online forum)	1

** For the purpose of determining the top three rank of the sources and to avoid redundancy, Websites and Googles, Yahoo or other search engines have been combined.

Q22: Please rank only three (3) of the most useful sources of your information security knowledge at home. (Most useful ← 1 2 3 → Least useful)

Sources of knowledge	Rank 1	Rank 2	Rank 3
Academic journals	16	4	10
Books	17	15	21
Daily newspaper	33	31	18
Websites and Search engines	135	116	80
Government or professional reports	2	5	1
Hearsay	8	13	17
Information discussions with colleagues, professional contacts	17	31	32

Interview	0	1	0
Magazines	14	27	24
Organisation's policy	2	3	5
Pamphlets/brochures	0	1	6
Posters	0	2	0
Presentation	5	3	2
Professional activities (conferences, meetings, briefings, etc)	1	5	14
Radio	1	12	6
Research articles	5	6	5
Television news	17	18	25
From what I learnt at my workplace	43	23	36
Other	10	2	3

Q23: How frequently do you read articles or news about information security at home?

Never: 96

Daily: 24

Weekly: 83

Monthly: 130

Q24: What is your opinion about giving your personal data on the web?

Absolutely secure: 12

Secure with terms and conditions given by the website: 148

Insecure even with the terms and conditions given by the website: 115

Absolutely insecure: 52

Other: 6

Other's detail(s)	No. of respondents
Depends on the website and the type of transactions	1
Do not know	1
Question terms not defined	1
I almost never add address and birth date to websites unless essential	1
Once information is given to other people, it is their choice to do whatever they want with the information	1

Depends on the who is asking 1

Q25: Do you back up the data on your personal computer (PC) periodically?
 Yes: 225
 No: 108

Q26: Do you use social networking websites like Facebook, Bebo, WAYN, or Friendster?
 Yes: 211
 No: 120
 I do not know what it is: 2

Q26A: What personal information have you made visible to others in your social networking websites?
 Real name: 124
 Email: 131
 Real date of birth: 95
 Full address: 17
 Phone number: 30
 Personal blog: 47
 Special occasions (e.g. birthday party, holiday, anniversary): 46
 Photographs of yourself: 142
 Photographs of your family members: 78
 Photographs of your friends: 88
 Photographs of your office: 14
 Photographs of your house: 16
 None of the above: 11
 Other: 3

Other's detail(s)	No. of respondents
Date of birth not without the year	1
Privacy is restricted to specified groups & my name / workplace can be Google anyway	1
My interests	1

Q27: What kind of security applications/controls you are using at home?

Security controls	Yes	No	I do not know
Antivirus	324	7	2
Firewall	252	63	18
Anti-phishing	139	122	72
Anti-spyware	242	58	33

Intrusion detection systems (IDS)	59	175	99
Spam filter	224	76	33

Q28: To what extent do the following statements apply to you? When using computer systems in my house....

Security Practices	Always	Sometimes	Never	Not applicable
I log off my computer whenever I leave a computer system	166	96	64	7
I backup my data on disks or CDs regularly	121	152	56	4
I check that antivirus software is enabled and updated	245	67	15	6
My passwords consists of at least 8 characters and uses the combination of letters (a-z), symbols (!@#\$\$%) and numbers (0-9)	198	85	42	8
I keep my password a secret and only I know it	242	65	18	8
I change my password regularly	73	142	109	9
I shred confidential documents before throwing them into the bin	150	89	80	14
I scan with antivirus any external disk/thumb drive/USB drive when first plugging it into the computer system	141	128	57	7
I report security incidents to the appropriate parties (e.g. Internet Service Provider (ISP), Computer Emergency Response Team (CERT) as soon as possible	81	97	129	26
I do download or install unauthorised copies of software	65	160	102	6
I do open and execute an executable file (.exe file) from an email attachment	38	110	180	5

I do click on hyperlinks in unsolicited/spam email messages and unknown websites	24	77	227	5
I look for "https://" or the "little gold padlock" before I make financial transactions online	209	74	34	16
I allow a web browser (e.g. Internet Explorer (IE)/Mozilla Firefox) to save my user id(s) and passwords for faster access in the future	69	134	126	4
I protect confidential files with passwords	108	132	84	9
I change the default password for my router	133	57	81	62
I use encryption key to protect my wireless connection	172	44	56	61
I read the privacy statement before I proceed with an action (such as registering with a website, installing an application or financial/online banking transaction)	126	160	44	3
I ensure nobody is looking at my keyboard each time I key in my password	157	98	57	21

Q29: If you have any suggestions for improving information security awareness training, please write in the space provided:

- 1) From my perspective, when a new employee joins a company, there is no security awareness training provided to them as an orientation. Security awareness among employees could improve drastically if the training is made compulsory for new employees
- 2) Make it as syllabus in school, treat it as an important stuffs.
- 3) the awareness program should be done in stages e.g. create awareness then step by step to introduce the activity that can be used/done by users to ensure information security.
- 4) Based on my experience, internet banking is the most important thing to highlight during security training
- 5) have a plan and get top managements commitment into it
- 6) publish security awareness in the newspaper
- 7) Organization enforcement in term of rules and regulations regarding information security in a workplace should be implemented.

- 8) Having comics of cartoons like what PhD comics is doing is a good idea to be included in the info sec awareness and training program because for me it is short, simple, easy to understand and good approach for people who prefer visual materials.
- 9) In an organization, give rewards to users who report security incidents to motivate others to do the same. Awareness training should be carried out at least once a year. Security Policy should be prepared and reviewed periodically. Government should encourage.
- 10) To communicate that it is available to all, it should be something everyone who uses a computer at work is taught and updated about.
- 11) Some people who are not very IT savvy need to be made aware of any issues using methods such as mail shots
- 12) probably make it in plain English so all levels of user understand
- 13) We need to have the course ware or lesson ware that attract user to really understand the security as a whole. Try to make them enjoy the lesson and make use of it. Try to build the awareness for school children as a target first. They are our future gene
- 14) There is currently no security awareness training - anything would be an improvement
- 15) I use MS Windows at work and Apple OS X at home so some of the specific work security issues/solutions etc are not relevant at home.
- 16) This prompted me to have a look and see if UoP offered any information security awareness training and I haven't been able to find any. So some would be an improvement
- 17) Information could be provided at staff induction / by line managers if not already done so. Perhaps some re-emphasis on the importance of information security awareness could be circulated / emailed to users. Explanation of jargon terms needs to be included.
- 18) know your insecurity so you can stay securely
- 19) For home use:- 1. training should include guidelines for choosing packages that do not slow up PC when running in background and ensuring that this remains the case (a. so that one is tempted to stop running and b. so that if PC is turned off the updates
- 20) Training and updated on information security awareness should be given by the company. I didn't know much about it, because I am not really it savvy. What I practice is based on what I learnt or heard from colleges and friends.
- 21) This should be compulsory for all employees as part of induction
- 22) We have to have more info about info security on TV
- 23) Create quiz about information security.
- 24) It would be good to have information security training, perhaps quarterly, so we can use the knowledge at home, where an IT department is not always on hand!
- 25) Never heard of information security awareness training before.
- 26) Media should aware with it, and provide fast access information to reduce the risk.
- 27) Free seminar/training with hands-on
- 28) Improving information security awareness with sharing with people and discussing is much better to spread the information.
- 29) It would be useful for information security awareness training with demos. Otherwise they might be too technical for non-IT people.

- 30) Make it more non-it savvy-friendly
- 31) Organisations should make sure that they conduct awareness training amongst its own staff. They should provide employee with original software, antivirus, firewall at client as well as server levels. IS should be implemented and documented for future r
- 32) Change the mindset of the people about security responsibilities.
- 33) Attitude must change
- 34) Supervisor sometimes do not allow to go to security training saying that not related to work
- 35) Maybe you should email the new development and other preventive measures to the user in the organisation directly every month/quarterly/half yearly to keep the awareness of IT security among the user.
- 36) You cannot train people to care about their internet security. Viruses, Trojans, spam etc morph at a fast rate. People need to care about their workstations, then only will they know how to protect themselves. Training needs to be fun, presentations, class
- 37) Make it easier or more user-friendly, approachable to pc-user-only (people who knows nothing @ minimum knowledge of computer technicality).
- 38) Latest Technology
- 39) Make it mandatory.
- 40) Hands on training should be at work place
- 41) Malaysian government should monitor information privacy and security in government agencies. There are such cases, information are sell to the third party.
- 42) Improving information security awareness training by using sms.
- 43) I think you need to include questions related to ISO 27000 series, CobIT or ITIL or something like that. Anyway the survey is look great ... hope you always success
- 44) There are different approaches for people like myself that used Open Source Software. At My Office OSCC MAMPU we are purely and fully using Ubuntu Linux as our Desktop and Server Operating System. The approach of protection is different for example, we do n
- 45) Catch them young, make security best practices a part of grade/high school computing classes.
- 46) Provide live demos instead of slides.

Appendix E

Pre-test Questions Version 1

Pre-Test Questions Version 1

Q1: Choose the **correct** matching statements:

- a) False Acceptance Rate = False Rejection Rate
- b) True Rejection Rate = False Non- Match Rate
- c) False Acceptance Rate = False Match Rate
- d) True Acceptance Rate = True Non-Match Rate

Q2: Below are three common measures of biometric accuracy that are very important for determining the final success of a system. Choose the **one** statement that is **not** a common measure:

- a) Equal Error Rate (EER)
- b) True Match Rate (TMR)
- c) Failure to Acquire Rate (FTA)
- d) Failure to Enrol Rate (FER)

Q3: The United Kingdom Biometrics Working Group has suggested a scheme for understanding relative biometric accuracy rates. What is the False Acceptance Rate for Medium security strength?

- a) 1 in 10 000/0.01%
- b) 1 in 100/1.0%
- c) 1 in 1,000,000/0.0001%
- d) 1 in 10/0.1%

Q4: Performance of a biometric system depends on:

- a) Accuracy
- b) Speed
- c) Failures to enrol
- d) All of the above

Q5: In the UK Passport Service study, which process takes longer to complete?

- f) Enrolment
- g) Verification
- h) Screening
- i) Transmission

Q6: Below are a number of true statements regarding False Rejection Rate (FRR). Which statement is **not** a true statement regarding False Rejection Rates (FRR)?

- a) A measure represents the frequency of cases where the legitimate user is rejected by the system.
- b) A measure represents the frequency of cases when biometric information is not matched against any records in a database where it should have
- c) Developers are trying to minimise this measure
- d) A measure represents the frequency of cases when biometric information from one person is correctly not matched to any records in a database

Q7: A Vitality test is also known as:

- a) Health and safety test
- b) Important test in a biometric enrolment
- c) A test that ensure the biometric sample is offered by a living person
- d) A test that ensure the accuracy of the biometric sample

Q8: According to a research conducted at George Washington University, the respondents prefer to use biometric technology for:

- f) Commercial, banking institution, travel and medical procedures
- g) Office physical access, air transportation screening, medical procedures and government functions
- h) Financial institution, medical procedures, commercial and government functions
- i) Banking institution, transportation screening, medical procedures and school

Q9: Who are more supportive in accepting biometric applications in commercial environments?

- a) Europeans
- b) Canadians
- c) Asians
- d) Americans

Q10: Why are users reluctant to accept biometric authentication? Choose **one** of the answers below.

- a) It is slightly easy to use compared to passwords
- b) They are not happy with the way the 'look and feel' of the systems
- c) They are not happy with the complexity of the system
- d) They are not happy with the a lot of pin that they have to memorise

Q11: Select the most important way to promote user acceptance of biometric systems.

- a) Inform them the cost of the system
- b) Inform them about the training that they will undergo to learn the system
- c) Inform them the maintenance after the system being deployed
- d) Inform them that their biometric image will be kept secret at all time

Q12: The biometric system is difficult to use because:

- a) Users lack of training
- b) Users have to remember their passphrase
- c) Users need to review their biometrics inputs each time they wanted to use the system
- d) User need to repeat twice every time they want to be authenticated

Q13: Biometrics technology uses computerised methods to identify a person by their unique _____ and _____ characteristics. Fill in the gaps.

- a) Human , physical
- b) Physical , behavioural
- c) Emotion , human
- d) Human , behavioural

Q14: 2D face recognition involves (Choose the best statement):

- a) Making unique measurements on how thick the user's face
- b) Making unique measurements on the temperature of human body
- c) Making unique measurements between key points on user's face
- d) Making unique measurement between the ridges of the user's face

Q15: Below are true statements regarding iris scanning. Choose the **one** statement which is **false**:

- a) Iris scanning measures patterns on the coloured part of the eye
- b) Iris scanners read from the outer edge towards the pupil, detecting and plotting the markings
- c) Iris scanning takes longer time to authenticate users
- d) Iris accuracy could be affected by objects obscuring the eye

Q16: Which of the condition(s) of the finger that might affect the fingerprint scanning process?

- a) Too wet
- b) Too dry
- c) All of the above
- d) None of the above

Q17: The corrugated _____ of the skin are non-continuous and form a pattern that has distinguishing features. Please fill in the blank with the appropriate word.

- a) Minutiae
- b) Ridges
- c) Pattern
- d) Image

Q18: Slap in biometrics refers to:

- a) A full image of user's backhand taken by simultaneously onto a scanner
- b) A full image of user's hand taken by simultaneously onto a scanner
- c) Fingerprints taken by simultaneously pressing all five fingers of one hand onto a scanner
- d) Fingerprints taken by simultaneously pressing four fingers of one hand onto a scanner

Q19: What are the five subsystems in a general biometric system?

- a) Data collection, presentation collection, signal processing, data storage and decision
- b) Data collection, signal processing, compression, data storage and decision
- c) Data collection, transmission, signal processing, data storage and decision
- d) Data collection, signal processing, segmentation, data storage, and decision

Q20: Which of the compression format below is **not** true?

- a) Facial images – Joint Photographic Experts Group
- b) Fingerprint – Wavelet Scalar Quantization
- c) Voice data – Code Excited Linear Prediction
- d) Hand geometry – Graphics Interchange Format

Q21: Choose the **best** definition for the term “enrolment”:

- a) Saving a template in the database every time a user scan his fingerprint
- b) Saving a template in the database for the first time a user scan his fingerprint
- c) Saving a template in the database when a user scan his fingerprint
- d) Saving a template in the database after a user has scan a few times

Q22: The primary purpose to obtaining biometric information from a collected sample of an individual’s physiological or behavioural characteristics is:

- a) Feature extraction
- b) Enrolment
- c) Segmentation
- d) Decision

Q23: Choose the correct statement about the decision to **reject** the claimed identity by a user.

- a) Any distance lower than the fixed threshold
- b) Any distance upper than the fixed threshold
- c) Any matched pattern that could not be acquired
- d) All of the above

Q24: Segmentation is defined as:

- a) The process of finding the biometric pattern within the transmitted signal
- b) The process of comparing a presented feature sample to the stored data
- c) The process of saving a template or a model into the database for the first time
- d) The process of compressing user data into before being transmitted

----- End of the Questions -----

Appendix F

Learning materials

Topic 1: Technical

Instruction: Read the text below.

GENERIC BIOMETRIC AUTHENTICATION

The generic system is divided into 5 subsystems: data collection, transmission, signal processing, decision and data storage. The whole system is presented in the figure below:

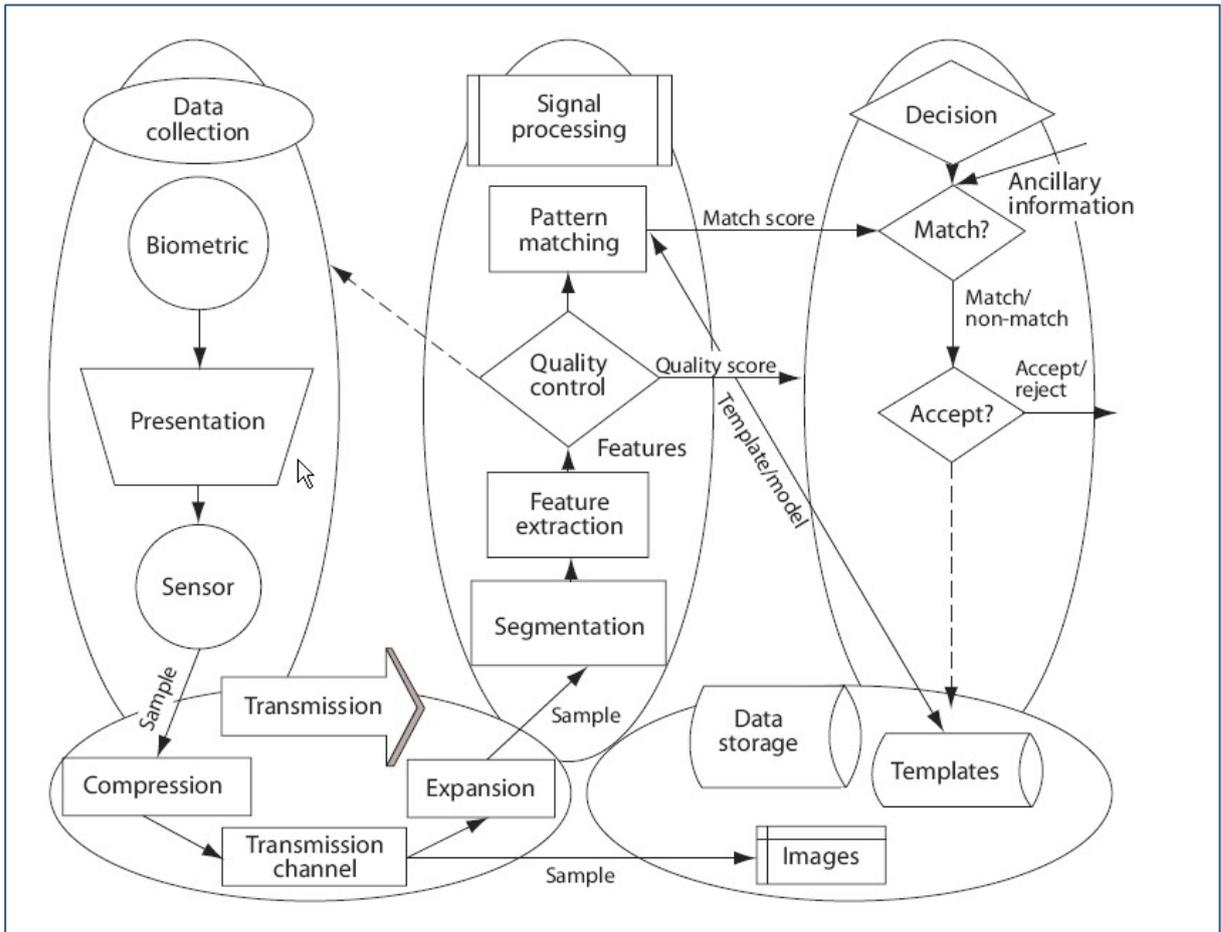


Figure 1: Generic biometric system

DATA COLLECTION

Biometric systems begin with the measurement of a behavioural/physiological characteristic. Key to all systems is the underlying assumption that the measured biometric characteristics are both distinctive between individuals and repeatable over time for the same individual. The problem is measuring and controlling these variations begins in the data collection subsystem. The user characteristic must be presented to a sensor. As already noted, the presentation of any biometric to the sensor introduces a behavioural component to every biometric method. Figure 2 below illustrates the component in the data collection subsystem.

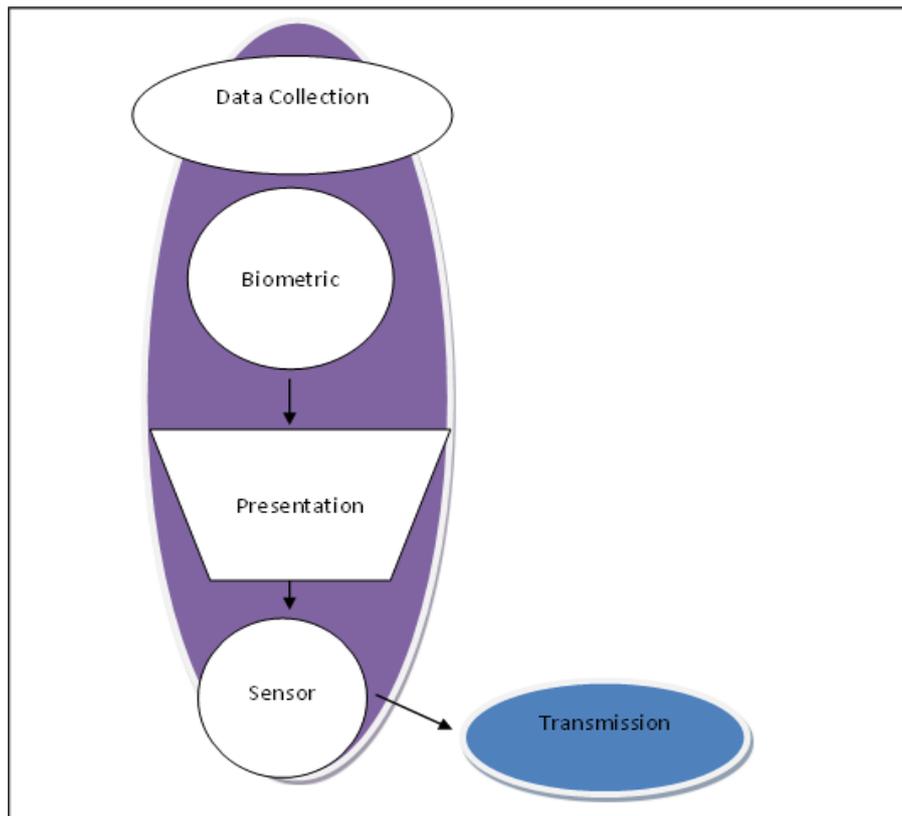


Figure 2 Data collection process

The output of the sensor, which is the input data upon which the system is built, is the convolution of:

- The biometric measure
- The way the measure is presented
- The technical characteristics of the sensor

Both the repeatability and the distinctiveness of the measurement are negatively impacted by changes in any of these factors.

If a system is to be open → the presentation + sensor characteristics must be standardised to ensure that biometric characteristics collected with one system will = to those collected on the same individual by another system.

If a system to be used in an overt, non-cooperative application → the user must not be able to wilfully change the biometric or its presentation sufficiently to avoid being matched to previous records.

TRANSMISSION

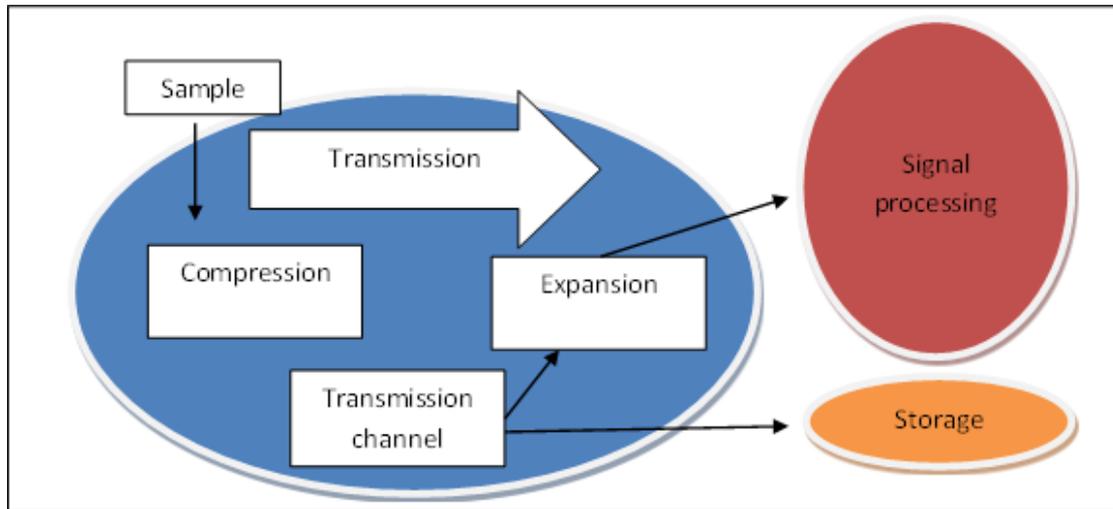


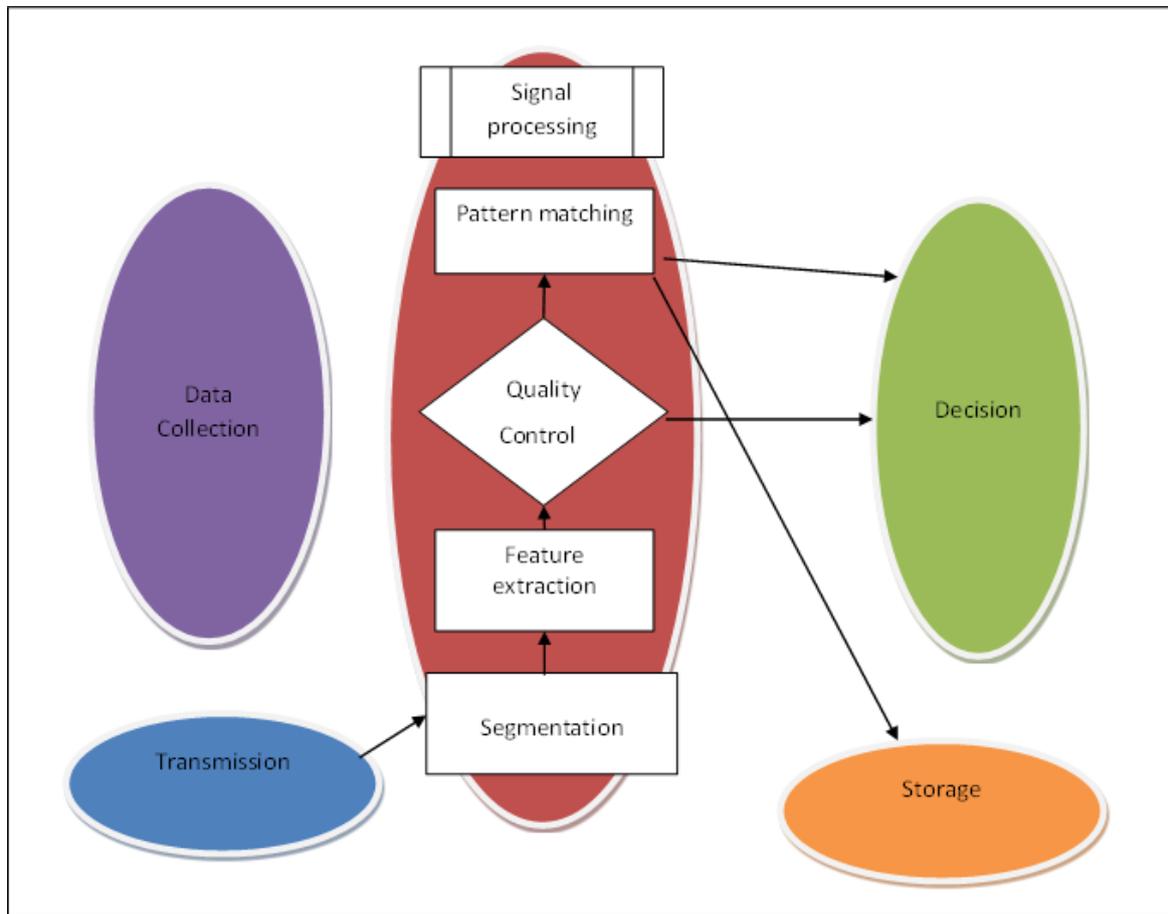
Figure 3 Transmission process

Some, but not all, biometric systems collect data at one location but store and/or process it at another. Such systems require data transmission.

If a great amount of data is involved, compression may be required before transmission or storage to conserve bandwidth and storage space.

Figure 3 shows compression and transmission occurring before the signal processing and image. In such cases, the transmitted or stored compressed data must be expanded before further use.

If a system to be open, compression and transmission protocols must be standardised so that every user of the data can reconstruct the original signal. Standard currently exist for the compression of fingerprint (Wavelet Scalar Quantization), facial images (JPEG), and voice data (Code Excited Linear Prediction).

SIGNAL PROCESSING**Figure 4 Signal processing process**

As shown in Figure 4, the signal processing subsystem is divided into 4 tasks:

Segmentation
 Feature extraction
 Quality control
 Pattern matching

- ❖ Segmentation is the process of finding the biometric pattern within the transmitted signal. For example, a facial recognition system must first find the boundaries of the face or faces in the transmitted image. Once the raw biometric pattern of interest has been found and extracted from larger signals, the pattern is sent to the feature extraction process.
- ❖ Feature extraction is fascinating. The raw biometric pattern, even after the segmentation from the large signal, contains non-repeatable distortions caused by the presentation, sensor and transmission processes of the system. These non-controllable distortions and any non-distinctive or redundant elements must be

removed from the biometric pattern, while at the same time preserving those qualities that are both distinctive and repeatable. These qualities expressed in mathematical form are called “features”. In a text-independent speaker recognition system for instance, we may want to find the features, such as the mathematical frequency relationships in the vowels, that depend only upon the speaker and not upon the words being spoken, the health status of the speaker, or the speed, volume and pitch of the speech.

In general, feature extraction is a form of non-reversible compression, meaning that the original biometric image cannot be reconstructed from the extracted features. In some systems, transmission occurs after feature extraction to reduce the requirement for bandwidth.

- ❖ After feature extraction, the quality of the signal received from the data collection will be checked. If the features are insufficient in some way, the received signal will be considered as defected and a new sample will be requested to the user while he/she is still at the sensor.

The feature “sample”, now of very small size compared to the original signal will be sent to the pattern matching process for comparison with one or more previously identified and stored feature templates or models. The feature in template = feature in sample. The term “model” is used to indicate the construction of a more complex mathematical representation capable of generating features characteristic of a particular user. Models and features will be of different mathematical types and structures. Models are used in some speaker and facial recognition systems. Templates are used in fingerprint, iris, and hand geometry recognition systems.

The term “enrolment” refers to the placing of a template or model into the database for the very first time. Once in the database and associated with an identity by external information (provided by the enrollee or others), the enrolment biometric data is referred to as the template or model for the individual to which it refers.

- ❖ The purpose of pattern matching process is to compare a presented feature sample to the stored data, and to send to the decision subsystem a quantitative measure of the comparison.

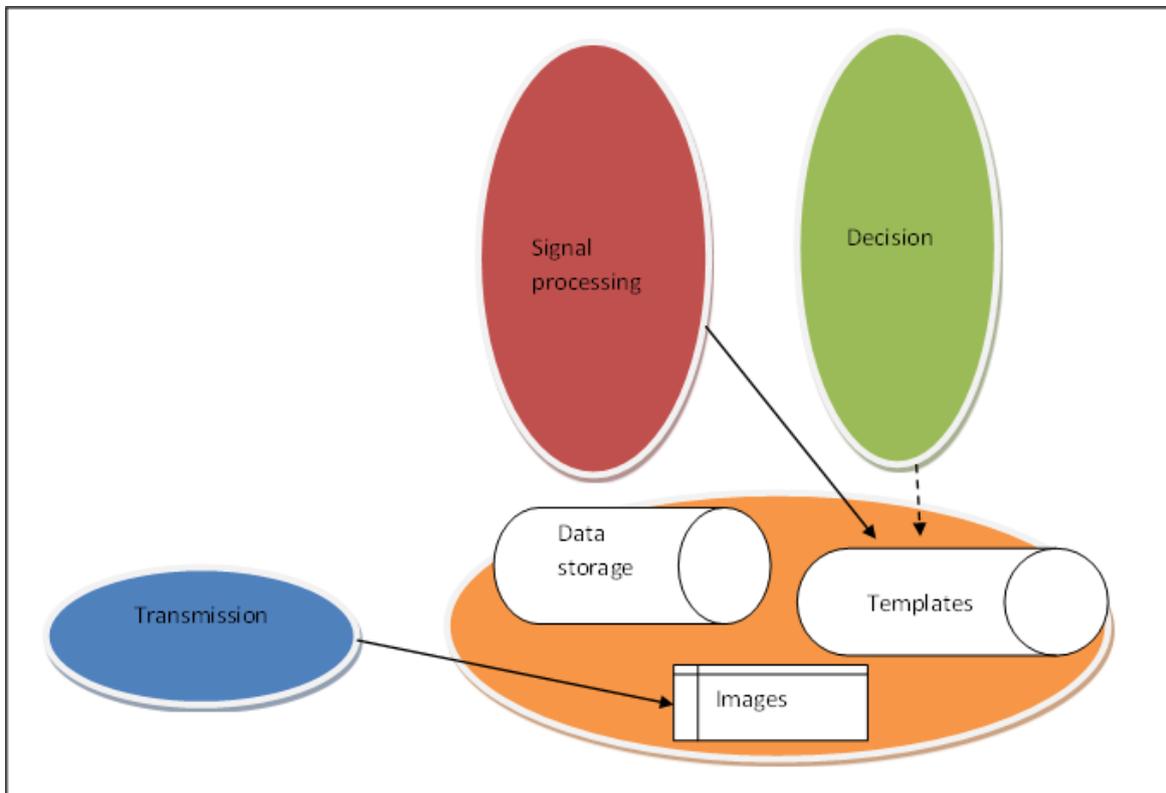
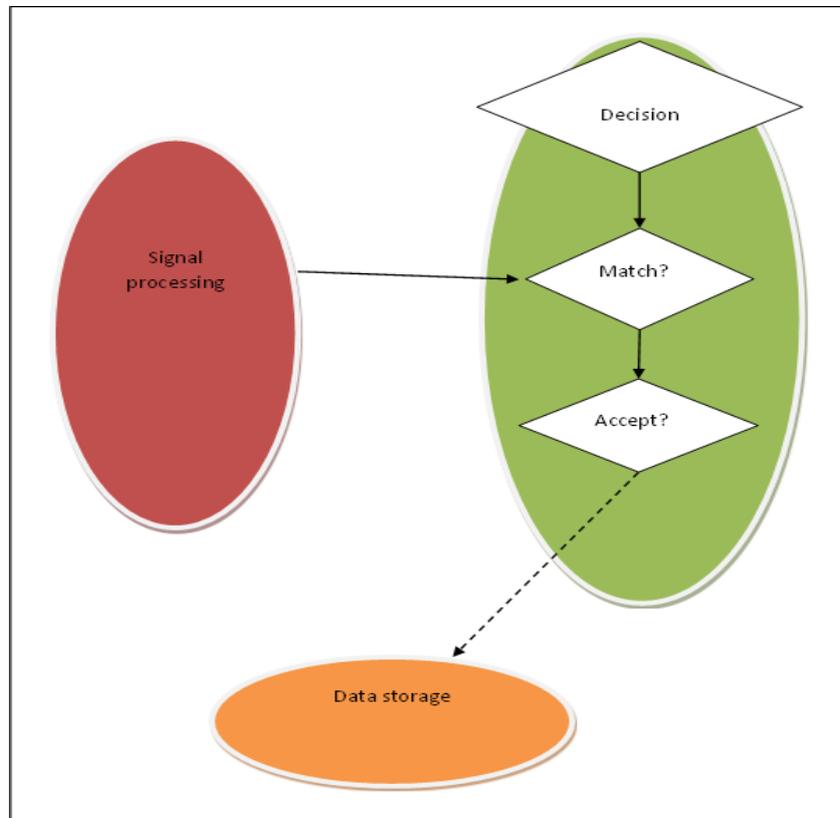
STORAGE

Figure 5 Storage process

The remaining subsystem to be considered is that of storage. Figure 5 shows the storage subsystem. There will be one or more forms of storage used, depending upon the biometric system. Templates or models from enrolled users will be stored in a database for comparison by the pattern matcher to incoming feature samples.

DECISION**Figure 6 Decision process**

The decision subsystem implements system policy by directing the database search, determines “matches” or “non-matches” based on the distance or similarity measures received from the pattern matcher, and ultimately makes an “accept/reject” decision based on the system policy. Figure 6 illustrate the decision subsystem.

Such a decision policy could be to reject the identity claim (either positive or negative) of any user whose pattern could not be acquired.

For an acquired pattern, the policy might declare a match for any distance lower than the fixed threshold and accept a user identity claim on the basis of this single match, or the policy could be declared a match for any distance lower than a user-dependent, time-variant, or environmentally linked threshold and require matches from multiple measures for an “accept” decision.

The policy could be to give all users, good guys and bad guys and bad guys alike, 3 tries to return a low distance measure and be accepted as matching claimed template. The decision policy employed is a management decision that is specific to the operational and security requirements of the system.

Topic 2 User Acceptance

Instruction: Double click on the icon below to listen to the file.



biometric.wma

For the purpose of reporting, below is the text for the sound clip above:

In one of the researches conducted by the George Washington University in the United States of America, more than fifty percent of the respondents accept the biometrics technologies for the user authentication. This is because they believe that biometrics would enhance security and accurate. The most widely accepted was fingerprints followed by iris recognition. Surprisingly, the lowest acceptance rate is signature recognition. The respondents prefer to use the technology for office building security, travel, air transportation screening, medical procedures, banking and financial institutions, and government functions.

On the other hand, about seven percents of the respondents did not agree to use the biometrics technology. Most of the respondents worry about their privacy issues being invaded if they use the technology. Research studies reported that users found biometrics to be less hygienic and more stressful than traditional PIN systems. Users have also reported significant fears that criminals may do harm to obtain the biometric (for example, cut their finger). Even though the users are informed on the 'vitality tests' that ensure the biometric is offered by a living person, this technology is still immature.

It appears that users are lack of understanding of biometrics templates. User only understands that their fingerprint is not a secret when the system saved the complete image of their fingerprints. They need to be assured that their fingerprint template will be kept secret at all time. This issue is very important in promoting user acceptance.

Previous research on user attitudes towards biometrics systems such as fingerprints to login into a computer and iris scan to pass through immigration checkpoints suggested that public has serious concerns about privacy and misuse. They often worried about their biometrics data could be lost, stolen or misused in some ways such as being framed using their fingerprint image for crime scenes. The research also highlighted that people are concerned about their biometrics information would be used by the government authorities in the ways that they did not approve.

Another study found that a majority of American fear that biometric systems will be vulnerable to criminals, misused by the government and used by the government to track their movements. Conversely, recent studies demonstrate that people are starting to accept the biometric systems. A survey of Canadian general public found that 80% of the respondents are considering of using biometric system in the next ten years.

Moreover, a report shows that people are accepting biometric systems for commercial applications, for instance, BioPay service. It is more likely there are factors being considered by users in accepting biometrics systems. These factors are associated with place, time activity that involved with users' biometrics information.

In terms of cultural context, researchers found that Canadians were more supportive of biometrics being included in passports than American. Nonetheless, Americans are more supportive of biometrics being used for commercial purposes. However, these cross-cultural studies are very limited and there is not enough evidence that shows cultural factors might affect the biometric deployment.

Another reason is the technology will cost them more money to be implemented. However, it is depending on which type of biometrics systems that being used. For example, fingerprint scanner will be cheaper as compared to a retina scanner.

In addition, they claimed that the technology is difficult to use. Proper user training will help to solve the biometrics complexity. Usually, users are expecting the system will identify them by swiping their fingerprints and scanning their eyes by intuition. However, these systems will only recognise if the user properly swipe as per system's instruction. Every biometric user must be trained and educated on how the technology works and what are the steps to be followed in order to use the system efficiently.

In conclusion, users are reluctant to accept biometrics due to the cost, complex usage, personal privacy and safety, even though they are aware of the advantages of using it.

Topic 3 Performance

Instruction: Read the text below.

THE STATE OF THE ART IN BIOMETRIC PERFORMANCE

1) Measuring biometric accuracy

One of the most important factors in the success of a biometric system is its accuracy. This is a measure of how well the system is able to correctly match the biometric information from the same person and avoid falsely matching biometric information from different people. The measurement of biometric accuracy is usually expressed as a percentage or proportion, with the data coming from simulations, laboratory experiments, or field trials. There are four main measures of biometric accuracy:

- 1-** True Acceptance Rate (TAR) / True Match Rate (TMR): this measure represents the degree that the biometric system is able to correctly match the biometric information from the same person. Developers of biometric systems attempt to maximise this measure.
- 2-** False Acceptance Rate (FAR) / False Match Rate (FMR): this measure represents the degree or frequency where biometric information from one person is falsely reported to match the biometric information from another person. Developers attempt to minimise this measure.
- 3-** True Rejection Rate (TRR) / True Non-Match Rate (TNMR): this measure represents the frequency of cases when biometric information from one person is correctly not match to any records in a database because, in fact, that person is not in the database. Developers attempt to maximise this measure.
- 4-** False Rejection Rate (FRR) / False Non-Match Rate (FNMR): this measure represents the frequency of cases when biometric information is not matched

against any records in a database when it should have been matched because the person is, in fact, in the database. Developers attempt to minimise this measure.

These measures of biometric accuracy are interdependent in biometric systems. First, there is a mathematical relationship between the corresponding true and false rates so that if one rate is known, the other can be calculated using $100\text{ percent} - X$ when working with percentages or $1.0 - X$ when working with proportions. For example, if the TMR is 98%, the FMR must be $100\% - 98\% = 2\%$.

Second, there is inevitably a trade-off where attempts to minimise the false matches of a system tend to decrease the frequency of true matches. System designers often have to adjust threshold values to get the best combination of true and false performance measures, and sometimes these adjustments are also available to customers who want to fine-tune their own biometric deployments.

There are three other common measures of biometric accuracy that are very important for determining the final success of a system, but they receive less attention:

Equal Error Rate (EER or ERR): the point at which the FAR is equal to FRR. This measure is often considered to be the optimal performance of a system where there is a reasonable trade-off between false acceptances and false rejections.

Failure to Enroll Rate (FER): the rate at which people are not able to enrol in a biometric system. Such failures are usually caused by missing or weak biometric characteristics, such as missing fingers, faint fingerprints, or an iris that is too dark. The FER is often an important, but overlooked, measure for determining the final business success of a biometric system because high FER will necessitate non-biometric alternatives so that people can still access the system or service without using the biometric system.

Failure to Acquire Rate (FTA): the rate at which biometric information is not obtained during use of a biometric system, even though the person was able to previously enrol. Failures to acquire can be caused by environmental conditions at the time of biometric system use, such as bad lighting affecting face or iris recognition systems, or dirty sensors affecting fingerprint systems. Failures to acquire are also important determinants of the final success of a biometric system, but they are often overlooked when discussing biometric accuracy.

2) Current data on biometric accuracy

Many vendors are eager to report that their systems are very accurate, since accuracy is seen as a key selling point and, as is shown below, there can be very large differences in the accuracy of different systems. One must be careful, however, when evaluating vendor's claims of accuracy because of the wide variety of methods that can be used to measure accuracy and known discontinuities between vendor claims and actual performance seen when the systems are deployed.

It is not clear what accuracy is required in actual practice. The nature of the information or systems being protected and the consequences of security failures have to be considered when determining the appropriate accuracy rates for a deployment scenario. The UK Biometrics Working Group has suggested a scheme for understanding relative biometric accuracy rates that is shown in Table 1. In many applications, basic or medium security strength may be all that is required to provide adequate protection.

FAR	FAR %	Strength
1 in 100	1.0	Basic
1 in 10,000	0.01	Medium
1 in 1,000,000	0.0001	High

Table 1: A scheme for understanding relative biometric strengths

The most reliable data on biometric accuracy comes from independent tests of a variety of vendor's systems. There have been a number of such tests conducted by government agencies such as National Institute of Standards and Technology (NIST) and Communications-Electronics Security Group (CESG). Typically, the vendors provide the biometric equipment and/or decision making algorithms and then have no further control of the tests. Thus, these independent tests are important when making calculations about probable biometric accuracy for any systems that might be deployed, although vendor-supplied numbers can also be used when appropriate.

3) Biometric speed

In addition to accuracy, the speed of operation of a biometric system will be important for its eventual success. If it takes too long to enrol and/or verify participants, the result will be frustrated users and slow business processes. The UK Passport Service study took a different approach and looked at the real time-time speed for verification, which included the time needed for the users' interaction with the biometric devices. This study found that it took an average of 1 minute and 13 seconds to perform the verification task, and disabled users were understandably slower (1 minute, 20 seconds).

The UK Passport study also measured the speed of enrolment. They found that it took an average of 3 minutes and 57 seconds to conduct a fingerprint enrolment, and again disabled participants were slower (4 minutes, 52 seconds). This enrolment time did include approximately 1 minute, 30 seconds of screening time where the new fingerprints were compared to the records in the existing database.

It is clear that any adopter of fingerprint systems will have to consider the time needed to enrol and verify people in the biometric system when they design their services and business processes. They would also have to be sensitive to individual differences that might lead to much longer times.

4) Failures to enrol

Failures to enrol are often a serious problem when deploying biometric systems, and yet they have not received as much as attention as matching failures. Failures to enrol can be caused by missing or damaged biometric characteristics, poor user training, poor devices and other reasons.

Topic 4 Modalities

Instruction: Please hold CTRL button and CLICK on the hyperlink below to watch the video.

<http://youtu.be/G7Crh5VK5YA>

Appendix G

Answer Key To The Pre-test Version 1

Answer to the pre and post test

- 1) C
- 2) B
- 3) A
- 4) D
- 5) A
- 6) D
- 7) C
- 8) B
- 9) D
- 10) C
- 11) D
- 12) A
- 13) B
- 14) C
- 15) C
- 16) C
- 17) B
- 18) D
- 19) C
- 20) D
- 21) B
- 22) A
- 23) D
- 24) A

Appendix H

Pre-test Questions Version 2

Respondent ID: _____

Pre-Test Questions

*Instruction: Please circle your answers. Choose only **one** answer for each question.*

Q1: Choose the **correct** matching statement:

- a) False Acceptance Rate = False Rejection Rate
- b) True Rejection Rate = False Non- Match Rate
- c) False Acceptance Rate = False Match Rate
- d) True Acceptance Rate = True Non-Match Rate
- e) False Acceptance Rate = True Non-Match Rate

Q2: Below are common measures of biometric accuracy that are very important for determining the final success of a system. Choose the **one** statement that is **not** a common measure:

- a) Equal Error Rate (EER)
- b) True Match Rate (TMR)
- c) Failure to Acquire Rate (FTA)
- d) Failure to Enrol Rate (FER)
- e) Equal Match Rate (EMR)

Q3: The United Kingdom Biometrics Working Group has suggested a scheme for understanding relative biometric accuracy rates. What is the False Acceptance Rate for Medium security strength?

- a) 1 in 10 000/0.01%
- b) 1 in 100/1.0%
- c) 1 in 1,000,000/0.0001%
- d) 1 in 10/0.1%
- e) 1 in 10,000,000/0.00001%

Q4: Performance of a biometric system depends on:

- a) Accuracy
- b) Speed
- c) Failures to enrol
- d) a, and b only
- e) a, b and c only

Q5: The following factors below should be considered when developing and implementing a biometric system **except**: (Choose only one answer)

- a) Time needed to enrol users' biometric characteristics
- b) Individual disabilities during the enrolment process
- c) Users' computer skills
- d) Users' training programme
- e) Privacy issues relating to system security

Q6: Below are a number of true statements regarding False Rejection Rate (FRR). Which statement is **not** a true statement regarding False Rejection Rates (FRR)?

- a) A measure that represents the frequency of cases where the legitimate user is rejected by the system.
- b) A measure that represents the frequency of cases where biometric information is not matched against any records in a database when it should have been
- c) Developers are trying to minimise this rate
- d) A measure that represents the frequency of cases where biometric information from one person is correctly not matched to any records in a database
- e) It is one of the measurements of biometric accuracy

Q7: A Vitality test is also known as:

- a) Health and safety test
- b) An important test of biometric enrolment
- c) A test that ensures the biometric sample has been offered by a living person
- d) A test that ensures the accuracy of the biometric sample
- e) A test to validate users' behavioural characteristics

Q8: What are people's concerns when using a biometrics system? (Choose only one answer)

- a) Loss of fingerprint and biometric data
- b) Their movements are tracked and misused by government
- c) System is not user friendly and they might be framed for a crime
- d) a and c only
- e) a, b and c only

Q9: Who are more supportive in accepting biometric applications in commercial environments?

- a) Europeans
- b) Canadians
- c) Asians
- d) Americans
- e) Africans

Q10: Why are users reluctant to accept biometric authentication? Choose **one** of the answers below.

- a) They like to use password authentication
- b) They are not happy with the 'look and feel' of the systems
- c) They are not happy with the complexity of the system
- d) They are not happy with a lot of pin numbers that they have to memorise
- e) They think that biometric authentication is not accurate

Q11: Select the **most** important way to promote user acceptance of biometric systems.

- a) Inform them of the cost of the system
- b) Inform them about the training that they will undergo to learn the system
- c) Inform them of the maintenance after the system has been deployed
- d) Inform them that their biometric image will be kept secret at all times
- e) Inform them that the system will be hassle-free all the time

Q12: Biometric systems are difficult to use because:

- a) Users lack of training
- b) Users have to remember their passphrase
- c) Users need to review their biometric inputs each time they wanted to use the system
- d) Users need to give their biometric samples twice every time they want to be authenticated
- e) Users need to ensure the time taken to scan their biometric sample is short

Q13: Biometrics technology uses computerised methods to identify a person by their unique _____ and _____ characteristics. Fill in the gaps.

- a) Human , physical
- b) Physical , behavioural
- c) Emotional , human
- d) Human , behavioural
- e) Emotional , physical

Q14: 2D face recognition involves (Choose the best statement):

- a) Making unique measurements on how thick the user's face is
- b) Making unique measurements on the temperature of the human body
- c) Making unique measurements between key points on the user's face
- d) Making measurements between the ridges of the user's face
- e) Making measurements between the minutiae of the user's face

Q15: Below are true statements regarding iris scanning. Choose the **one** statement which is **false**:

- a) Iris scanning measures patterns on the coloured part of the eye
- b) Iris scanners read from the outer edge towards the pupil, detecting and plotting the markings
- c) Iris scanning takes a longer time to authenticate users
- d) Iris scanning accuracy could be affected by objects obscuring the eye
- e) Iris scanning is accurate and reliable

Q16: Which condition(s) of the finger might affect the fingerprint scanning process?

- a) Too wet
- b) Too dry
- c) Injured finger
- d) c only
- e) a, b and c only

Q17: The corrugated _____ of the skin are non-continuous and form a pattern that has distinguishing features. Please fill in the blank with the appropriate word.

- a) Surface
- b) Ridges
- c) Pattern
- d) Image
- e) Facade

Q18: Slap in biometrics refers to:

- a) A full image of the back of a user's hand taken by a scanner
- b) A full image of a user's hand taken by a scanner
- c) Fingerprints taken by simultaneously pressing all five fingers of one hand onto a scanner
- d) Fingerprints taken by simultaneously pressing four fingers of one hand onto a scanner
- e) Fingerprints taken by simultaneously pressing both of a user's hands onto a scanner

Q19: What are the five subsystems in a general biometric system?

- a) Data collection, presentation collection, signal processing, data storage and decision
- b) Data collection, signal processing, compression, data storage and decision
- c) Data collection, transmission, signal processing, data storage and decision
- d) Data collection, signal processing, segmentation, data storage, and decision
- e) Data collection, transmission, segmentation, data storage and decision

Q20: Which of the compression format below is **not** true?

- a) Facial images – Joint Photographic Experts Group
- b) Fingerprint – Wavelet Scalar Quantization
- c) Voice data – Code Excited Linear Prediction
- d) Hand geometry – Graphics Interchange Format
- e) Iris images – Joint Photographic Experts Group

Q21: Choose the **best** definition for the term “enrolment”:

- a) Saving a template in the database every time a user scans their fingerprint
- b) Saving a template in the database the first time a user scans their fingerprint
- c) Saving a template in the database when a user scans their fingerprint
- d) Saving a template in the database after a user has scanned their fingerprint a few times
- e) Saving a template in the database for future uses

Q22: The primary approach of obtaining biometric information from a collected sample of an individual's physiological or behavioural characteristics is:

- a) Feature extraction
- b) Enrolment
- c) Segmentation
- d) Decision
- e) Transmission

Q23: Choose the correct statement about the decision to **reject** the claimed identity of a user.

- a) Any measurement lower than the fixed threshold
- b) Any measurement above the fixed threshold
- c) Any matched pattern that could not be acquired
- d) a and c only
- e) a, b and c only

Q24: Segmentation is defined as:

- a) The process of finding the biometric pattern within the transmitted signal
- b) The process of comparing a presented feature sample with stored data
- c) The process of saving a template or a model into the database for the first time
- d) The process of compressing user data before being transmitted
- e) The process of comparing presented user data with stored data

Appendix I

Answer Key to Pre-test Version 2

Answer to the pre and post test

- 1) C
- 2) E
- 3) A
- 4) E
- 5) C
- 6) D
- 7) C
- 8) E
- 9) D
- 10) C
- 11) D
- 12) A
- 13) B
- 14) C
- 15) C
- 16) E
- 17) B
- 18) D
- 19) C
- 20) D
- 21) B
- 22) A
- 23) E
- 24) A

Appendix J

Faculty of Science and Technology Ethical Approval of Research

Involving Human Participants

PLYMOUTH UNIVERSITY
FACULTY OF SCIENCE AND TECHNOLOGY

Human Ethics Committee

APPLICATION FOR ETHICAL APPROVAL OF RESEARCH INVOLVING
HUMAN PARTICIPANTS

All applicants should read the guidelines at the end of this application

This is a WORD document. Please complete in WORD and extend space where necessary.

*All applications must be word processed. Handwritten applications **will** be returned.*

One signed hard-copy must be sent to Paula Simson. You may also send an unsigned electronic copy of your application to paula.simson@plymouth.ac.uk as this will speed up the review process

1. TYPE OF PROJECT

1.1 What is the type of project? (Tick 1 only)

STAFF should tick one of the three options below:

Specific project

Tick this box if you are seeking approval for a specific study, or set of studies, with methods that are explained fully in the following sections. This form of approval is appropriate for funded projects with a clear plan of work and limited duration.

Thematic programme of research

Tick this box if you are seeking approval for a programme of work using a single paradigm. This form of approval is appropriate for pilot work, or routine work that is ethically straightforward. Note, the maximum period of approval for thematic ethical clearance is 3 years.

Practical / Laboratory Class

Tick this box if you are seeking approval for a teaching activity which involves student involvement in the role of an experimental participant.

1.2 Tick 1 only

POSTGRADUATE STUDENTS should tick one of the options below:

Taught Masters Project

M.Phil / PhD by research

UNDERGRADUATE STUDENTS should tick one of the two options below:

Student research project



Practical / Laboratory class where you are acting as the experimenter

2. APPLICATION

<p>2.1 TITLE of Research project</p>
<p>Improving Information Security Awareness</p>
<p>2.2 General summary of the proposed research for which ethical clearance is sought, briefly outlining the aims and objectives and providing details of interventions/procedures involving participants (no jargon)</p>
<p>Information security awareness has become importance as more people are using the Internet in their daily activities. Ranging from shopping, communicating and even socialising are now being done via the Internet. In relation to that, public should be aware on the possible threats and dangers in dealing with the information being shared through the networks. To improve the awareness, people should be educated such as through the awareness program. The current information security programs are one size fits all. In the educational area, learning styles approach is used to tailor-made teaching materials to suit students' learning preferences.</p> <p>Since it is useful to adopt learning styles in educating students, the research is designed to find people learning preferences for information security topics. The study also designed to find whether people can learn efficiently if they were being taught in the way that they prefer; in this study, learning styles Visual, Aural, Reading/Writing and Kinaesthetic (VARK). The teaching materials in the study are tailor-made for the four different learning styles.</p> <p>Appropriate participants for this study are individual age 18 years and older, and does not have a formal education in information security.</p> <p>This data collection session will require participants to complete a set of the VARK learning styles questionnaire, a pre-test, go through learning materials, a short survey and a post-test. The learning materials were created and presented in the way that portrays the four different ways (visual, aural, reading and kinaesthetic) of teaching biometrics topics.</p>

2.3 Physical site(s) where research will be carried out
User will undergo the data collection session in the Centre for Security Communications and Network Research (CSCAN) test bed in room A304, Portland Square.
2.4 External Institutions involved in the research (e.g. other university, hospital, prison etc.)
n/a
2.5 Name, telephone number, e-mail address and position of lead person for this project (plus full details of Project Supervisor if applicable)
<ol style="list-style-type: none">1. Shuhaili Talib (Research student) – shuhaili.talib@plymouth.ac.uk, +4417525862872. Dr. Nathan L. Clarke (Director of Studies) – n.clarke@plymouth.ac.uk +4417525862183. Prof Steven Furnell (Second Supervisor) - steven.furnell@plymouth.ac.uk, +441752586234

2.8 Start and end date for research for which ethical clearance is sought (NB maximum period is 3 years)

Start date: November 2011
2011

End date: Mid December

2.9 Name(s) of funding source(s) if any

n/a

2.10 Has funding already been received?

n/a **No**

In-part

Yes

2.11 Has this same project received ethical approval from another Ethics Committee?

n/a

No

Yes

2.12 If yes, do you want Chairman's action?

n/a

No

Yes

If yes, please include other application and approval letter and STOP HERE. If no, please continue

3. PROCEDURE

3.1 Describe procedures that participants will engage in, Please do not use jargon

- 7 Respondent will be given a consent form with details of research information. They will read and understand the procedure before they proceed with the study. If they agreed, they will give their signature.
- 8 The researcher will give the research information sheet to respondent to give the ideas on what they are going to do in the study.
- 9 Once the respondent is ready, the respondent will use a laptop provided by the researcher and starts with Part I: Learning Styles VARK questionnaire. They will complete the questionnaire online, and upon completion, the researcher will record the results in a secured database in the laptop.
- 10 In Part II: Pre-test, the researcher will give a hardcopy of the pre-test, which consists of 24 multiple-choice questions (MCQ) to be completed.
- 11 Respondent will be given a 3 minutes break before continuing to the next part.
- 12 In Part III: Learning materials, respondent will go through the learning materials in the laptop. The respondent will read texts and diagrams, listen to a short lecture and watch a video in the session.
- 13 Part IV: User experience survey, respondents will be given a short survey consists of 6 MCQ to share their thoughts and experience on the learning materials and also demographic information.
- 14 Finally, Part V: Post-test, respondent will be given a hardcopy of 24 MCQ to be completed to assess what they have learnt from the learning materials.

3.2 How long will the procedures take? Give details

The whole experiment will take approximately 60 minutes. The breakdown of the average time taken by users are as below:

Part I: Learning styles VARK questionnaires – approximately 5 – 8 minutes

Part II: Pre-test – approximately 17 minutes

- The 3 minutes break will be given to participant before proceed with the next part.

Part III: Learning materials – approximately 28 minutes

Part IV: User experience survey – approximately 3 minutes

Part V: Post-test – approximately 10 minutes

3.3 Does your research involve deception?

No <input checked="" type="checkbox"/> Yes <input type="checkbox"/>
3.4 If yes, please explain why the following conditions apply to your research: n/a
a) Deception is completely unavoidable if the purpose of the research is to be met
n/a
b) The research objective has strong scientific merit
n/a
c) Any potential harm arising from the proposed deception can be effectively neutralised or reversed by the proposed debriefing procedures (see section below)
n/a
3.5 Describe how you will debrief your participants
<p>Respondents will be given consent form and research information sheet before they are able to start with this study. After they have read, understand and agree to participate, they will give their signature on consent form. Then, they will be given a guidance sheet; the step by step instructions to help users to understand what they are going to experience in the experiment. The principal researcher will be with the participants at all time during the experiment; given them chance to ask if they do not understand or facing any problems. The information regarding confidentiality and right to withdraw has already mentioned in the forms. Should participants want to know how they have performed, access to individual results will be provided once analysed and upon a request.</p>

3.6 Are there any ethical issues (e.g. sensitive material)?
No <input checked="" type="checkbox"/> Yes <input type="checkbox"/>
3.7 If yes, please explain. You may be asked to provide ethically sensitive material. See also section 11
n/a

4. BREAKDOWN OF PARTICIPANTS

4.1 Summary of participants

Type of participant	Number of participants
<i>Non-vulnerable Adults</i>	30/40 participants
<i>Minors (< 16 years)</i>	n/a
<i>Minors (16-18 years)</i>	n/a
<i>Vulnerable Participants (other than by virtue of being a minor)</i>	n/a

<i>Other (please specify)</i>	n/a
TOTAL	30/40 participants

4.2 How were the sample sizes determined?
This study would expect approximately target participants to be at least 30 respondents to facilitate a meaningful analysis. 30 participants will be considered sufficient baseline because some other similar research which has been conducted using the same sample size.
4.3 How will subjects be recruited?
The subjects will be recruited via email, predominantly targeting the non-computing students in Plymouth University and colleagues in Faculty of Science and Technology. Having said that, Centre for Security, Communications and Network Research (CSCAN) and International Student Advisory Service websites will advertise the study as well. A news entry on the staff/student portal will also be requested. If any users are interested, they will be given the details of the research project as aforementioned in section 3.1.
4.4 Will subjects be financially rewarded? If yes, please give details.
Yes, an amount of £10 will be awarded per participant.

5. NON-VULNERABLE ADULTS

5.1 Are some or all of the participants non-vulnerable adults?
No <input type="checkbox"/> Yes <input checked="" type="checkbox"/>
5.2 How will participants be recruited? Name any other institution(s) involved

The subjects will be recruited via email, predominantly targeting the non-computing students in Plymouth University and colleagues in Faculty of Science and Technology. Having said that, Centre for Security, Communications and Network Research (CSCAN) and International Student Advisory Service websites will advertise the study as well. A news entry on the staff/student portal will also be requested.

5.3 Inclusion / exclusion criteria

Respondents who are 18 years old and above, who does not have formal education in information security, agree and understand all procedure able to take part in this study.

5.4 How will participants give informed consent?

Respondents are able to quit or withdraw at any time.

(Please refer to the research information sheet)

5.5 Consent form(s) attached

No

Yes

If no, why not?

n/a

5.6 Information sheet(s) attached

No <input type="checkbox"/>	Yes <input checked="" type="checkbox"/>
<i>If no, why not?</i>	
n/a	
<i>5.7 How will participants be made aware of their right to withdraw at any time?</i>	
<p>The right for participants to withdraw at any time is stated in consent form and research information sheet.</p> <p>(Please refer to the research information sheet)</p>	

5.8 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?

With regards to the confidentiality, responses are collected and stored in a secure database on researcher's computer without containing any identifying information. The information from the study may be used in future journal publications and conference presentation. However, data and references to any participants will be anonymised so that the true identities are not revealed.

6. MINORS <16 YEARS

6.1 Are some or all of the participants under the age of 16?

No Yes

If yes, please consult special guidelines for working with minors. If no, please continue.

6.2 Age range(s) of minors

n/a

6.3 How will minors be recruited? (See guidelines). Name any other institution(s) involved

n/a

6.4 Inclusion / exclusion criteria

n/a

6.5 How will minors give informed consent? Please tick appropriate box and explain (See

guidelines)
n/a Opt-in <input type="checkbox"/> Opt-out <input type="checkbox"/>
6.6 Consent form(s) for minor attached
n/a No <input type="checkbox"/> Yes <input type="checkbox"/>
If no, why not?
n/a
6.7 Information sheet(s) for minor attached
n/a No <input type="checkbox"/> Yes <input type="checkbox"/>
If no, why not?
n/a
6.8 Consent form(s) for parent / legal guardian attached
n/a No <input type="checkbox"/> Yes <input type="checkbox"/>
If no, why not?
n/a

7.2 How will minors be recruited? (See guidelines). Name any other institution(s) involved
n/a
7.3 Inclusion / exclusion criteria
n/a
7.4 How will minors give informed consent? (See guidelines)
n/a
7.5 Consent form(s) for minor attached
n/a No <input type="checkbox"/> Yes <input type="checkbox"/>
If no, why not?
n/a
7.6 Information sheet(s) for minor attached
n/a No <input type="checkbox"/> Yes <input type="checkbox"/>
If no, why not?
n/a

8.1 Are some or all of the participants vulnerable? (See guidelines)
No <input checked="" type="checkbox"/> Yes <input type="checkbox"/>
<i>If yes, please consult special guidelines for working with vulnerable groups. If no, please continue.</i>

8.2 Describe vulnerability (apart from possibly being a minor)
n/a

8.3 How will vulnerable participants be recruited? Name any other institution(s) involved
n/a

8.4 Inclusion / exclusion criteria
n/a

8.5 How will participants give informed consent?
n/a

8.6 Consent form(s) for vulnerable person attached
n/a No <input type="checkbox"/> Yes <input type="checkbox"/>

If no, why not?

n/a
8.7 Information sheet(s) for vulnerable person attached
n/a No <input type="checkbox"/> Yes <input type="checkbox"/>
If no, why not?
n/a
8.8 Consent form(s) for parent / legal guardian attached
n/a No <input type="checkbox"/> Yes <input type="checkbox"/>

<i>If no, why not?</i>
n/a
<i>8.9 Information sheet(s) for parent / legal guardian attached</i>
n/a No <input type="checkbox"/> Yes <input type="checkbox"/>
<i>If no, why not?</i>
n/a
<i>8.10 How will participants be made aware of their right to withdraw at any time?</i>
n/a
<i>8.11 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?</i>
n/a

9. EXTERNAL CLEARANCES

Investigators working with children and vulnerable adults legally require clearance from the Criminal Records Bureau (CRB)

9.1 Do ALL experimenters in contact with children and vulnerable adults have <u>current</u> CRB clearance? Please include photocopies.
No <input type="checkbox"/> Yes <input type="checkbox"/> N/A <input checked="" type="checkbox"/>
9.2 If no, explain
n/a
9.3 If your research involves external institutions (school, social service, prison, hospital etc) please provide cover letter(s) from institutional heads permitting you to carry out research on their clients, and where applicable, on their site(s). Are these included?
No <input type="checkbox"/> Yes <input type="checkbox"/> N/A <input checked="" type="checkbox"/>
If not, why not?
n/a

10. PHYSICAL RISK ASSESSMENT

**10.1 Will participants be at risk of physical harm (e.g. from electrodes, other equipment)?
(See guidelines)**

No

Yes

10.2 If yes, please describe

n/a

10.3 What measures have been taken to minimise risk? Include risk assessment proformas.

n/a

10.4 How will you handle participants who appear to have been harmed?

n/a

1. PSYCHOLOGICAL RISK ASSESSMENT

11.1 Will participants be at risk of psychological harm (e.g. viewing explicit or emotionally sensitive material, being stressed, recounting traumatic events)? (See guidelines)

No Yes

11.2 If yes, please describe

n/a

11.3 What measures have been taken to minimise risk?

n/a

11.4 How will you handle participants who appear to have been harmed?

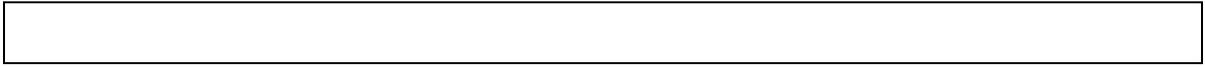
n/a

12. RESEARCH OVER THE INTERNET

12.1 Will research be carried out over the internet?
No <input type="checkbox"/> Yes <input checked="" type="checkbox"/>
12.2 If yes, please explain protocol in detail, explaining how informed consent will be given, right to withdraw maintained, and confidentiality maintained. Give details of how you will guard against abuse by participants or others (see guidelines)
<p>The right for participants to withdraw at any time is stated in consent form and research information sheet.</p> <p>(Please refer to the research information sheet)</p> <p>Participants will only be using the Internet connection for:</p> <ul style="list-style-type: none">a) Part I: Learning Styles VARK questionnaire. The participant will answer a set of 16 multiple-choice questions and get their results online. The result will be recorded by the principle researcher into a secured user database in the researcher's computer.b) Part III: Learning Materials. The participants will be given a video link that could be viewed via YouTube link. The video will only contain learning materials that relevant to the biometrics topic. <p>The principle researcher will guide and be with the participant during the whole experiment.</p>

13. CONFLICTS OF INTEREST & THIRD PARTY INTERESTS

13.1 Do any of the experimenters have a conflict of interest? (See guidelines)
No <input checked="" type="checkbox"/> Yes <input type="checkbox"/>
13.2 If yes, please describe
n/a
13.3 Are there any third parties involved? (See guidelines)
n/a No <input type="checkbox"/> Yes <input type="checkbox"/>
13.4 If yes, please describe
n/a
13.5 Do any of the third parties have a conflict of interest?
n/a No <input type="checkbox"/> Yes <input type="checkbox"/>
13.6 If yes, please describe
n/a



14. ADDITIONAL INFORMATION

14.1 [Optional] Give details of any professional bodies whose ethical policies apply to this research

n/a

14.2 [Optional] Please give any additional information that you wish to be considered in this application

n/a

--

15. ETHICAL PROTOCOL & DECLARATION

To the best of our knowledge and belief, this research conforms to the ethical principles laid down by the Plymouth University and by any professional body specified in section 14 above.

This research conforms to the University’s Ethical Principles for Research Involving Human Participants with regard to openness and honesty, protection from harm, right to withdraw, debriefing, confidentiality, and informed consent

Sign below where appropriate:

STAFF / RESEARCH POSTGRADUATES

	Signature	Date
Principal Investigator: _____	_____	
Other researchers: _____	_____	
_____	_____	
_____	_____	

Staff and Research Postgraduates should send the completed and signed copy of this form to Paula Simson, Secretary to the Science and Technology Human Research Ethics Committee, A106 Portland Square.

UG / TAUGHT POSTGRADUATES

Signature

Date

Student:

Supervisor / Advisor:

Undergraduate and Taught Postgraduate students should pass on the completed and signed copy of this form to their School Representative on the Science and Technology Human Ethics Committee.

Signature

Date

School Representative on Science and
Technology Faculty Human Ethics Committee

SAMPLE SELF-CONSENT FORM

UNIVERSITY OF PLYMOUTH

FACULTY OF SCIENCE AND TECHNOLOGY

Human Ethics Committee Sample Consent Form

CONSENT TO PARTICIPATE IN RESEARCH PROJECT / PRACTICAL STUDY

Name of Principal Investigator

Title of Research

Brief statement of purpose of work

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

I understand that the Principal Investigator of this work will have attempted, as far as possible, to avoid any risks, and that safety and health risks will have been separately assessed by appropriate authorities (e.g. under COSHH regulations)

Under these circumstances, I agree to participate in the research.

Name:

Signature:

Date:

SAMPLE INFORMATION SHEET FOR ADULT / CHILD

UNIVERSITY OF PLYMOUTH

FACULTY OF SCIENCE AND TECHNOLOGY

RESEARCH INFORMATION SHEET

Name of Principal Investigator

Title of Research

Aim of research

Description of procedure

Description of risks

Benefits of proposed research

Right to withdraw

If you are dissatisfied with the way the research is conducted, please contact the principal investigator in the first instance: telephone number *[PI tel. number here]*. If you feel the problem has not been resolved please contact the secretary to the Faculty of Science and Technology Human Ethics Committee: Mrs Paula Simson 01752 584503.

Faculty of Science and Technology Human Research Ethics Committee List of School Representatives

School of Psychology Prof Chris Harris (Chair)

Prof Judy Edworthy

School of Geography, Earth and Environmental Sciences Dr Rupert Hodder

Dr Sanzidur Rahman

School of Biomedical & Biological Sciences Dr David J. Price

School of Marine Science & Engineering Dr Matthew Barlow

School of Computing & Mathematics Mr Martin Beck

External Representative Dr Jane Grose

Lay Member Rev. David Evans

Committee Secretary: Mrs Paula Simson

email: paula.simson@plymouth.ac.uk

Tel: 01752 584503

Appendix K

VARK Questionnaire

The VARK Questionnaire (Version 7.1)

How Do I Learn Best?

Choose the answer which best explains your preference and circle the letter(s) next to it.

Please circle more than one if a single answer does not match your perception.

Leave blank any question that does not apply.

1. You are helping someone who wants to go to your airport, town centre or railway station. You would:

- a) go with her.
- b) tell her the directions.
- c) write down the directions.
- d) draw, or give her a map.

2. You are not sure whether a word should be spelled 'dependent' or 'dependant'. You would:

- a. see the words in your mind and choose by the way they look.
- b. think about how each word sounds and choose one.
- c. find it in a dictionary.
- d. write both words on paper and choose one.

3. You are planning a holiday for a group. You want some feedback from them about the plan. You would:

- a. describe some of the highlights.
- b. use a map or website to show them the places.
- c. give them a copy of the printed itinerary.
- d. phone, text or email them.

4. You are going to cook something as a special treat for your family. You would:

- a. cook something you know without the need for instructions.
- b. ask friends for suggestions.
- c. look through the cookbook for ideas from the pictures.
- d. use a cookbook where you know there is a good recipe.

5. A group of tourists want to learn about the parks or wildlife reserves in your area. You would:

- a. talk about, or arrange a talk for them about parks or wildlife reserves.
- b. show them internet pictures, photographs or picture books.

- c. take them to a park or wildlife reserve and walk with them.
- d. give them a book or pamphlets about the parks or wildlife reserves.

6. You are about to purchase a digital camera or mobile phone. Other than price, what would most influence your decision?

- a. Trying or testing it.
- b. Reading the details about its features.
- c. It is a modern design and looks good.
- d. The salesperson telling me about its features.

7. Remember a time when you learned how to do something new. Try to avoid choosing a physical skill, eg. riding a bike. You learned best by:

- a. watching a demonstration.
- b. listening to somebody explaining it and asking questions.
- c. diagrams and charts - visual clues.
- d. written instructions – e.g. a manual or textbook.

8. You have a problem with your heart. You would prefer that the doctor:

- a. gave you a something to read to explain what was wrong.
- b. used a plastic model to show what was wrong.
- c. described what was wrong.
- d. showed you a diagram of what was wrong.

9. You want to learn a new program, skill or game on a computer. You would:

- a. read the written instructions that came with the program.
- b. talk with people who know about the program.
- c. use the controls or keyboard.
- d. follow the diagrams in the book that came with it.

10. I like websites that have:

- a. things I can click on, shift or try.
- b. interesting design and visual features.
- c. interesting written descriptions, lists and explanations.
- d. audio channels where I can hear music, radio programs or interviews.

11. Other than price, what would most influence your decision to buy a new non-fiction book?

- a. The way it looks is appealing.
- b. Quickly reading parts of it.
- c. A friend talks about it and recommends it.
- d. It has real-life stories, experiences and examples.

12. You are using a book, CD or website to learn how to take photos with your new digital camera. You would like to have:

- a. a chance to ask questions and talk about the camera and its features.
- b. clear written instructions with lists and bullet points about what to do.
- c. diagrams showing the camera and what each part does.
- d. many examples of good and poor photos and how to improve them.

13. Do you prefer a teacher or a presenter who uses:

- a. demonstrations, models or practical sessions.
- b. question and answer, talk, group discussion, or guest speakers.
- c. handouts, books, or readings.
- d. diagrams, charts or graphs.

14. You have finished a competition or test and would like some feedback. You would like to have feedback:

- a. using examples from what you have done.
- b. using a written description of your results.
- c. from somebody who talks it through with you.
- d. using graphs showing what you had achieved.

15. You are going to choose food at a restaurant or cafe. You would:

- a. choose something that you have had there before.
- b. listen to the waiter or ask friends to recommend choices.
- c. choose from the descriptions in the menu.
- d. look at what others are eating or look at pictures of each dish.

16. You have to make an important speech at a conference or special occasion. You would:

- a. make diagrams or get graphs to help explain things.
- b. write a few key words and practice saying your speech over and over.
- c. write out your speech and learn from reading it over several times.
- d. gather many examples and stories to make the talk real and practical.

The VARK Questionnaire Scoring Chart

Use the following scoring chart to find the VARK category that each of your answers corresponds to. Circle the letters that correspond to your answers:

e.g. If you answered b and c for question 3, circle V and R in the question 3 row.

Question a category b category c category d category

3 K V R A

Scoring Chart

Question a category b category c category d category

1 K A R V

2 V A R K

3 K V R A

4 K A V R

5 A V K R

6 K R V A

7 K A V R

8 R K A V

9 R A K V

10 K V R A

11 V R A K

12 A R V K

13 K A R V

14 K R A V

15 K A R V

16 V A R K

Calculating your scores

Count the number of each of the VARK letters you have circled to get your score for each VARK category.

Total number of Vs circled =

Total number of As circled =

Total number of Rs circled =

Total number of Ks circled =

Appendix L

User Experience Survey

Section A: Learning Experiences Questionnaire

Q1: Please rank the groups of learning strategies below: (Most preferred ← 1 2 3 4 → Least preferred)

- a) Videos/field trips/teaching others _____
- b) Books/reports/notes/lists _____
- c) Podcasts/attend discussions/discuss topics with others _____
- d) Diagrams/graphs/maps/symbols _____

Note: Please answer the following questions with regards to your experiences with the learning materials that you have go through in this experiment.

Q2: Please rank the topics below based on your interests, regardless of how the topics being presented. (Most Interested ← 1 2 3 4 → Least Interested)

- a) Topic 1: Technical _____
- b) Topic 2: User Acceptance _____
- c) Topic 3: Performance _____
- d) Topic 4: Modalities _____

Q3: Please rank the topics below based on the way they were being presented. (Most preferred ← 1 2 3 4 → Least preferred)

- a) Topic 1: Technical (Visual) _____
- b) Topic 2: User Acceptance (Aural) _____
- c) Topic 3: Performance (Reading/Writing) _____
- d) Topic 4: Modalities (Kinaesthetic) _____

Q4: Please rank the following topics based on the difficulty level. (Most Difficult ← 1 2 3 4 → Least Difficult)

- a) Topic 1: Technical _____
- b) Topic 2: User Acceptance _____
- c) Topic 3: Performance _____
- a) Topic 4: Modalities _____

Q4: Please write comments and suggestions (if any) in the box provided.

Part B: Demographics

Q1: Please select your gender:

- a) Male
- b) Female

Q2: To what age group do you belong?

- a) 16-24
- b) 25-34
- c) 35-44
- d) 45-54
- e) 55+

Q3: What is your highest level of education?

- a) School
- b) College
- c) Undergraduate
- d) Postgraduate
- e) Doctorate
- f) Other (Please specify) _____

Thank you

=====**End of Questionnaire**=====

Appendix M
Expert Evaluation

A: Observation on the PISE functions

PISE has provided several functions for enabling trainees to Function

Dashboard

Add new users

Name address email password/confirm password

Select learning style – Combination of visual, aural, kinaesthetic / read and write

Manage

Update

Verify

Assign

Create account for the new users – the interface and expectation to users are clearly specified.

Learning styles are briefly explain to guide the users e.g. visual, read/write, aural and kinaesthetic

The steps to be done by the users are clearly labelled and the tasks to be done by the users in sequence – pretest – learning- assessment and finally result.

The questions are arranged in sequence and users will be able to choose the answer easily from the radio button.

In additions, the main page of PISE – clearly indicate how to navigate to home, personalised learning plan, upload related file and changing profile. Logout button or icon is clearly located on the top right of the screen.

Result of the pretest are clearly shown and also the post test result are clearly - the learning style is clearly identified based on given question so the users will be given the appropriate question according the correct and expected module shown on the result page. Results are displayed on the overall statistic of who have taken the test. Result shown for module 1 and module 2. Incomplete users also shown.

In learning module, the visual mode was design to show for private and public trainee download the module option e.g. Module 1 – V1, Module 2 – V2 and Module 3 – V3 are clearly shown and design for the trainee. The download function is clearly indicated by the common icon 'download'. The trainee can share the module with other through the upload function.

For the system administrator, the administrator will be able to monitor the registered users for private trainee or public trainee. The status of users can be easily identified from the label or bar chart that separates the group of users by active users or pending users. The administrator has the authority to approve or reject the pending users based on the required qualification. In additional, the administrator has the responsibility to assign the role for the users – a user can be a private or public trainee or training course administrator.

Additionally the administrator can manage the users by deleting or changing the users roles. Administrator also can assign the learning module to the users according to the performance of the users.

The administrators can edit and delete the learning module when required. Finally the administrator is capable to verify the assessment result.

B: Evaluation on the PISE user interface

The PISE (Personalising Information Security Education) has delivered the overall functions for enabling the trainees to identify their learning style through a pre-test. Then, the trainees could learn the Information Security training materials by the modules. The module is assigned by the learning style and verified by the administrator. The administrator is given several tasks to monitor the categories and performances of the trainees. The trainees' roles could be reassigned by the administrator when needed. The administrator is given an access to amend the learning module according to the new

requirements and delete the modules when obsolete. The administrator is also responsible to verify assessment result.

The overall PISE design of the interface and navigation are easy to learn and use. The appearance and layout of the interface are consistent, sophisticated but simple and easy to navigate. Furthermore, the colours selected for the interface are well blended and easy on the eyes of the users. The menus and icons are clearly designed and easy to be identified by the trainees when performing the task. In the registration interface, there is only minimum information is required by the system therefore it simplifies the task to register as a user or trainee.

The trainees could decide to be the public or private users, then the administrator is provided with a simple interface, which consists of three radio button to approve the type and status of the trainees. All the functions are labelled step by step so the trainees are guided in the in the overall process of getting the personalised learning module for Information security. As soon as the pre-test is completed, the result of learning style is clearly displayed to the trainees, then they can proceed to the next steps. The module then will be assigned according to the learning style. The administrator interface shows the functions clearly such as approving the trainees status, removing or amending the learning module. Finally, the reports for status of trainees (approved or pending, private or public, administrator) are stated clearly and easy to be identified by the administrator. The verification function for the assessment is also simple and easy to perform. Overall, PISE has fulfil the basic main objective as a system that enable trainees to learning the information security module according to their learning style. For enhancement, more function could be added such as email notification for verification, categorisation according to level of knowledge of the trainees (e.g. novice or expert).

Appendix N
Publications

An Analysis of Information Security Awareness within Home and Work Environments

Shuhaili Talib^{1,2}, Nathan L. Clarke^{1,3}, and Steven M. Furnell^{1,3}

¹Centre for Security, Communications and Network Research (CSCAN), University of Plymouth, Plymouth, PL4 8AA, United Kingdom
{shuhaili.talib, n.clarke, s.furnell}@plymouth.ac.uk

²International Islamic University Malaysia, Kulliyah of ICT, Department of IS, P.O. Box 10, 50728, Kuala Lumpur, Malaysia

³School of Computer and Information Science, Edith Cowan University, Perth, Western Australia

Abstract - As technology such as the Internet, computers and mobile devices become ubiquitous throughout society, the need to ensure our information remains secure is imperative. Unfortunately, it has long been understood that good security cannot be achieved through technical means alone and a solid understanding of the issues and how to protect yourself is required from users. Whilst many initiatives, programs and strategies have been proposed to improve the level of information security awareness, most have been directed at organizations, with a few national programs focused upon home users. Given people's use of technology is primarily focused upon those two areas: the workplace and home, this paper seeks to understand the knowledge and practice relationship between these environments. Through the survey that was developed, it was identified that the majority of the learning about information security occurred in the workplace, where clear motivations, such as legislation and regulation, existed. It was also found that user's were more than willing to engage with such awareness raising initiatives. From a comparison of practice between work and home environments, it was found that this knowledge and practice obtained at the workplace was transferred to the home environment. Given this positive transferability of knowledge and the willingness to learn about how to remain secure, an opportunity exists to move away from specific organizational awareness programs and to move towards awareness raising strategies that, whilst deployed in the organization, will develop an all-round individual security culture for users independent of the environment within which they are operating.

Keywords-information security; information security awareness; security culture; security management

Introduction

The volume and nature of information security threats has evolved, moving away from technical savvy hackers demonstrating their skill, to organized and well established crackers that aim to receive substantial financial rewards for their efforts [1]. This has resulted in an increase in cybercrime activities and subsequent threats end-users find themselves the target of. For examples, [2] stated that 52% of organizations had encountered threats in 2007.

Another survey [3] found that 64% of respondents had encountered a Phishing email – a threat rarely encountered 5 years ago. To safeguard users a range of security countermeasures exist. These tools continually evolve in sophistication and increase in number to counter the changing nature of the threats. However, in order for these to operate successfully they inherently rely upon the end-user to be able to deploy, configure and operate them. Unfortunately, it is also a well recognized fact that security is only as strong as the weakest link; and the weakest link is frequently the end-user [4].

To counter the threat caused by end-users an increased focus has been given towards information security awareness and the need to educate and inform end-users. Within an organizational context, efforts towards improving awareness amongst employees have increased with [5] indicating 82% of Enterprise organizations having training programs. Unfortunately, however, this is not necessarily the case for all, with [6], which largely comprises of small-to-medium sized companies (SMEs), indicating only 40% of their respondents conduct training. Whilst many organizations arguably have the resources to provide such training, should they deem it important to do so, they only represent a (95%) proportion of people who use the Internet. The remaining users are typically home-users or the general public. Worryingly, evidence demonstrates that it is this group of users that are most at risk, with 95% of all attacks being focused upon them [7]. Home users have a variety of resources at their disposal in order to improve their awareness of online threats. All the major Anti-Virus providers, Operating System vendors and government initiatives such as [8-10] all provide supporting information to the home user.

Whilst training programs and initiatives exist within both the workplace and home, little research has been conducted to understand what is being taught and where, the effectiveness of such strategies and to what degree learning styles play a role in achieving good information security practice. Information security awareness can be tackled from a variety of different directions, such as within school, government-sponsored initiatives and security providers; however, this paper will specifically focus upon and investigate the behavior, practices and interactions within and between organizations and home environments. The paper is organized as follows: Section II discusses the current state-of-art

in information security awareness and the development of security culture. Section III describes the methodology of the study, with section IV presenting the results. Section V discusses the main findings of the study with the conclusion and future work being presented in Section VI.

Prior work in information security awareness training

Information security awareness has been given an increasingly important focus within both academic and commercial communities. Organizations are gradually understanding the importance of their information assets and developing strategies to improve awareness throughout the company. Good corporate governance, regulation and legislation have also helped in raising the importance and relevance of good information security policies and practices [11]. Within academia, focus by researchers has partially moved away from the technical issues towards understanding the end user and developing models and programs that organizations can utilize in developing better awareness [12]. Interestingly, within academia, current research is suggesting that simple awareness strategies that educate employees about particular security topics through traditional mechanisms such as class-room based teaching, online education and poster/email campaigns are not sufficient in maintaining long-term information security practice [13-14]. Rather an increasing volume of research is proposing the need to develop an information security culture within the organization – moving away from surface learning and embedding or indoctrinating good practice within employees [14, 15-17]. The authors of these studies believe through establishing an information security culture in the organization, long-term security practice can be maintained and moreover, the drive towards awareness and education of security issues becomes self-fulfilling, as employees are engaged and proactive about their practice.

Within the context of home users, awareness raising initiatives have been created. Reference [8] is a UK Government sponsored initiative that provides a blanket based approach; providing general information about the risks and how to get protected. The site provides a variety of information from beginnings guides to specific information about relevant threats in a timely fashion. The site is predominately text based information with the addition of occasional video files. Other countries such as the USA have similar national based websites [9]. A number of companies that provide security software and operating systems also provide web-based access to resources – largely reading based – to assist in educating and informing home users [18-19].

Arguably, motivating home users into undertaking security training is challenging as security is always a requirement but never actually the primary task the user is trying to achieve. People often do not have the understanding they need to do it and moreover for those that do, they frequently do not have the time or inclination in any case. Worryingly, evidence demonstrates even when users do think they know about security and how to protect themselves, this is often found not to be the case. A joint study by [20] found that while 75% of home users thought they had spam protection, in fact only 42% actually did. This disparity between what they think they have and actually do have illustrates a significant gap in their understanding.

In order to achieve good security awareness considerable research has been undertaken into developing various learning mechanisms,

such as: face-to-face training sessions, email messages, online training, video game, intranet-based access and poster campaigns [21-25]. Whilst focus has been given to what and how to educate within organizations, research has identified the importance of measuring the effectiveness of such programs in order to ensure education leads to practice [26-27]. The Computer Security Institute (CSI) survey reported that 68% of the organizations measure the effectiveness of their awareness training [5]. Unfortunately, no figures were given as to the actual levels of effectiveness of the training. Various approaches have been identified to assist in creating an effective security program, such as, having more user engagement in the process through workshops and providing the training on a continuous basis. [12, 28-29].

However, whilst such strategies might be possible for organizations to utilize, home users would find it arguably difficult to engage for a multitude of reasons: desire, time, resources and the knowledge they need to, to name but a few. Unfortunately, there is little evidence demonstrating whether home users are in fact knowledgeable about information security and indeed practicing it.

A survey of end-user awareness and practices

Given the prior literature in the area, it was concluded that it was difficult to determine the effectiveness of training and moreover where and how they received that training. In addition, whilst it could be hypothesized that the majority of training came from organizations, it is not clear exactly to what extent learning from work and home played a role in information security practice in general. A survey was therefore created to assess these factors. A quantitative method of collecting data was chosen for the study in order to maximize the number of respondents across a broad spectrum of industries and roles. The aims of the survey are:

- To understand respondents general levels of security awareness and practice.
- To understand whether they received training from work and if so, what type and how effective it was.
- To understand the relationship between knowledge gained and practice between work and home
- To understand how people learn and what preferences they have towards various learning styles.

The survey consists of four sections: Demographics; Information Security Awareness; Practice at Workplace and Practices at Home. The Practices at Workplace, sought to investigate the current practice of respondents at their workplace. The section also enquired about the type of training that they have attended and what the learning methods that they have experienced had been and what they preferred. Respondents were also asked about the sources of information security knowledge in the workplace. This section provided information about the degree of transferability of information security knowledge between home and the workplace. At the end of the section is a list of common security practices that have been created to understand what their practices at their workplace actually are. The final section on Practices at Home sought to mirror much of the composition of the

previous section but with a view to practices and education at home.

The survey was distributed to a wide range of people regardless of location but with the condition that they were in employment and regularly use a computer at home and their workplace. The study was undertaken from 20th August – 7th October 2008 (49 days). The survey collection has been stopped when it reached more than the survey target (300) respondents. The survey was promoted via email, based on the authors' academic contacts, personal contacts, from the word-of-mouth and two mailing lists such as Google and Yahoo groups. A total of 333 responses were obtained and the results are analyzed in the sections that follow.

RESULTS

An analysis of the demographics identified that a fairly even split in responses were received from both genders (55% male; 45% female). It was found that the majority of the respondents (55%) were from the age group 25 to 34 and 81% had at least an undergraduate level of education. This could be due to the personal contacts of the author and those who are in the age group are more likely to be IT literate and have at least an email account. Whilst this proportion of users are clearly not representative of the general population, it is not felt this would bias the results of the survey except to provide perhaps a more informed and educated response to the questions. The results therefore probably indicate a more positive perspective on the use and knowledge of information security than what exists within the general population.

Information Security Awareness

In order to assess the level of security awareness, respondents were asked to rate their perceived level against a five point scale. Almost half of them (49%) rated themselves at high or very high (as illustrated in Fig. 1). When tied to the question asking respondents what their level of competency is with Information Technology (IT), where 64% stated that they had at least an advanced level of knowledge, it can be surmised that this group of respondents are well educate and informed about IT and Information Security in general.

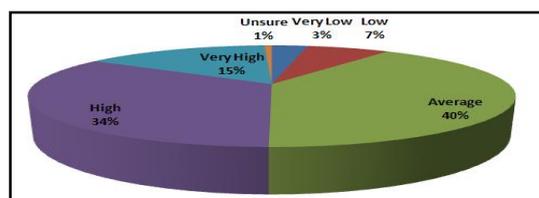


Figure 1. Perceived level of information security awareness.

In order to better understand what aspects of information security respondents understood, they were asked a couple of questions surrounding their knowledge of security threats and their use of social networking sites. Table I presents the results of respondent's awareness of a variety of security threats. Un-surprisingly, the long-standing threats such as Virus and Spam were amongst the highest selected as being understood and newer threats such as zero-day attacks, Botnets and Zombies less understood. Interestingly, whilst 70% understood Phishing, a relatively smaller 44% understood Social Engineering, of which Phishing is an

example of. The list of terms also included a couple of fake terms – Phlopping and Whooping – so that it was possible to identify respondents who might be exaggerating their knowledge or providing arbitrary responses. On the whole, relatively small numbers (7-10%) of respondents thought they had heard and understood the terms. That said it is a little concerning that these terms received any acknowledgement at all.

TABLE I. PERCEIVED UNDERSTANDING OF SECURITY THREATS

Information Security Terms	You Understand It (%)	You Never Heard Of It (%)
Virus/Worm	92	0
Trojan horse	80	3
Spam	90	0
Social engineering	44	24
Phishing	70	10
Pharming	24	42
Identity theft	81	8
Key loggers	57	22
Phlopping ^a	7	68
Botnets	33	43
Zombies	33	38
Denial of service	56	24
Packet sniffer	47	37
Whooping ^a	10	59
Hacker	95	1
Zero day attacks	29	44
Cracker	56	24

a. Fake security term

Social networking is a popular Internet activity, which literature has suggested is a common threat vector when looking to obtain information about people for subsequent use in identity fraud [30-32]. Amongst the respondents, 63% indicated they belong to one or more sites. When asked what information they release onto the social network, the respondent group overall appear to be informed and careful about releasing too much information. Table II illustrates that whilst 59% and 62% are releasing information regarding their real name and email address; only 7% reveal their full postal address. The most worrying statistic is the 45% releasing their date of birth but along with their name this amount of information is unlikely to result in identity theft.

TABLE II. PERSONAL INFORMATION REVEALED BY SOCIAL NETWORKING

Personal Information	You understand it (%)
Real name	59
Email	62

Personal Information	You understand it (%)
Real date of birth	45
Full address	8
Phone number	14
Personal blog	22
Special occasions	22
Photographs of yourself	67
Photographs of your family members	37
Photographs of your friends	42
Photographs of your office	7
Photographs of your house	8
None of the above	5
Other	1

Information Security Practices at Workplace

Analysing the participant's responses with reference to their practices within work, 36% stated their organization provided some sort of training with regards to information security. When comparing this to the size of the organization the respondent works for, it was found that 36% came from SMEs and coincidentally 36% also came from Enterprises (an Enterprise being defined as those organizations with 250 or greater employees). Whilst this figure is in line with the 40% stated by [6], which largely canvases SMEs, it falls somewhat short of [5] survey results; 80% (whose respondents are largely but not exclusively Enterprises). A further analysis of those responding on behalf of Enterprises shows that relatively few (3%) come from US-based companies – where regulation and legislation have arguably been prime motivators in ensuring staff are appropriately trained. Of the 36% of respondents who stated their organization provided training, 95% also stated they attended the training sessions.

In order to understand more about security practices in the workplace, respondents were asked about the sources of their information security knowledge. The top three information security sources at work are presented in Table 3; with websites and search engines the most popular. Arguably this could be due to many organizations now providing open access to the Internet. This freedom permits the employee to search and locate information of value at the time required. In addition to asking what their top three sources of information security knowledge were, they were also asked what they prefer. Interestingly, the results from these two questions came out identically, illustrating user's already have the freedom of choice when it comes to learning about information security and organizations are not burdening them with approaches they would not prefer.

From Table III, it is evident that much of the knowledge for Information Security within a workplace comes from fairly informal means – web searches and informal discussions with colleagues. Interestingly, these results do illustrate the importance

and relevant of the organizational policy in informing employees and moreover practice.

TABLE III. TOP THREE SOURCES OF INFORMATION SECURITY & LEARNING AT WORK

Top Three For Information Security In The Workplace		Top Three Most Preferred Sources For Information Security In The Workplace	
1	Websites and search engines	1	Websites and search engines
2	Informal discussions with colleagues and professional contacts	2	Information discussions with colleagues and professional contacts
3	Organization's policy	3	Organization's policy

This freedom of choice of how to learn comes through again when the respondents were asked about where or how they received their training. 28% of respondents responded that it was through self-study. As illustrated in Fig. 2, the remaining options received a fairly even split, indicating that if organizations are willing to invest in training their staff, the methods utilized will vary with no single option being a considered standard. Interestingly, further analysis of these responds when taking into account the size of the organization found that the preferred training type was independent of the organizational size, with SMEs willing to invest in outside experts as much as Enterprises – countering the standard assumption that SMEs do not have the resources to pay for training and would rely upon less expensive options such as self-study or online training.

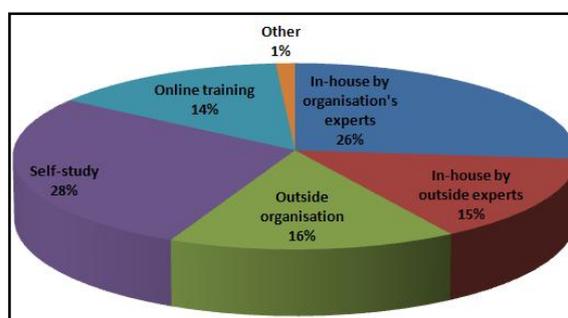


Figure 2. Preferred training type.

Respondents were also asked how frequent they would like to have security training. As Fig. 3 illustrates, the largest proportion of users preferred to have an on-demand service, with the majority of the remaining respondents split between monthly, quarterly, half-yearly and yearly. Overall 95% of respondents felt they needed some level of training.

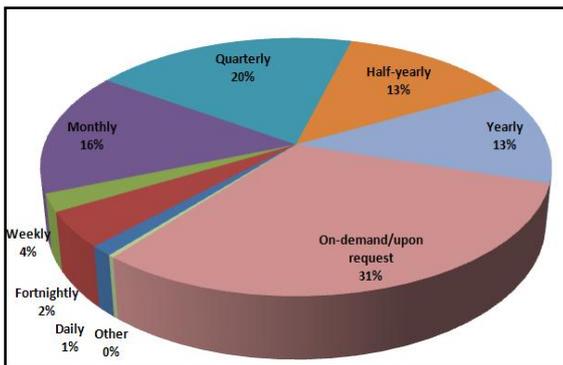


Figure 3. Respondent preference to having information security training.

Information Security Practices at Home

In order to compare practice from the workplace and home, respondents were asked a series of questions with respect to their practice at home. When analysing the top three sources of acquiring information security knowledge and what sources they preferred to learn from, it can be seen that the lists were identical, with web searches coming out first, what they had learnt from the workplace second, and reading newspapers and magazines third (as illustrated in Table IV). Upon reflection, this correlation should be expected as within the home environment you have complete freedom over what and how you learn. The user is not forced through employment to attend training courses or learn in a specific manner depending upon how the organization has decided to implement training. This freedom provides the user with the opportunity of using learning approaches that are preferred and most convenient to the individual. Arguably, without the formal training approaches that organizations utilize it is difficult to understand the depth of learning that goes on at home – with much of the learning likely being a result of news articles and press coverage of a particular event. A further research that focused on the level of understanding of information security knowledge acquired at home would be required to further explore on this aspect.

TABLE IV. TOP THREE SOURCES OF INFORMATION SECURITY & LEARNING AT HOME

Top Three For Information Security At Home		Top Three Most Preferred Sources For Information Security At Home	
1	Websites and search engines	1	Websites and search engines
2	From what I learnt at my workplace	2	From what I learnt at my workplace
3	Daily newspaper and Magazines	3	Daily newspaper

That said, the results from Table IV do illustrate the users are willing and do learn at home. Interestingly, the second most preferred source of information is what they learn from the workplace. Acquiring knowledge about information security within

the workplace has an impact upon the level of awareness and learning at home.

In addition to understanding how they learn, respondents were also asked how frequent that learning takes place. Fig. 4 presents the breakdown of responses. 71% of respondents undertake some level of training at home with 39% performing this on average on a monthly basis and 25% weekly. Whilst the regularity of the training is somewhat infrequent, given the lack of motivation within the home environment to undertake training, it is encouraging to note that over two thirds are willing to undertake some level of training at home.

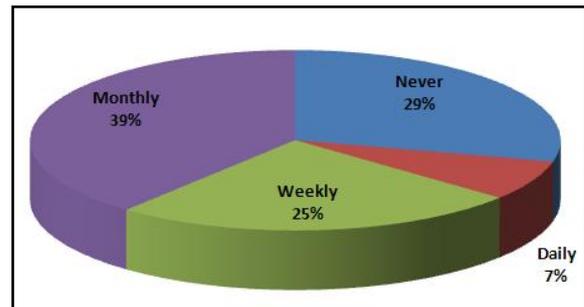


Figure 4. How frequent learning takes place at home.

Given that the proportion of users not willing to learn at home and the proportion that learn on a monthly basis make up 68% of the respondents, the need to acquire the knowledge necessary to ensure they remain secure at home is imperative. Arguably therefore, the knowledge users obtain within the workplace and subsequently transfer into the home environment is key to establishing a level of information security awareness for many respondents. Without such transference, a good proportion of home users will have little or no security awareness.

Effectiveness of Information Security Training

Having established training practices at home and the workplace, the survey proceeded to understand the extent to which this training and practice was effective. A total of 115 of the total respondents received training, 115 did not and the remaining claimed that they are not sure they have attended the training. Whilst training, awareness and practice are arguably associated with each other, simply undertaking training or having an awareness of an issue does not necessarily imply practice. To this end, Fig. 5 provides a comparison between those respondents who undertook training and what they considered their level of security awareness is. A total of 67% of respondents who undertook training felt they had a high or very high level of awareness. This compares to just 43% who had not received training. This demonstrates respondents at least perceive they have a better understanding of the information security threats and countermeasures over those that have not received training.

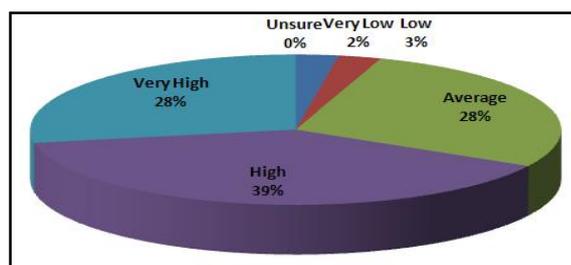


Figure 5. Respondents who attended training and their awareness level.

TABLE V. PERCEIVED UNDERSTANDING OF SECURITY THREATS BASED UPON WHETHER TRAINING HAD BEEN PROVIDED

Information Security Terms	Respondents Who Received Training (%)	Respondents Who Did Not Receive Training (%)
Virus/Worm	97	93
Trojan horse	94	77
Spam	94	88
Social engineering	58	40
Phishing	81	67
Pharming	34	20
Identity theft	85	81
Key loggers	72	55
Phlopping ^a	10	5
Botnets	50	28
Zombies	50	30
Denial of service	75	56
Packet sniffer	65	48
Whooping ^a	17	8
Hacker	97	95
Zero day attacks	45	23
Cracker	73	55

a. Fake security term

A further analysis of respondents' understanding of various security threats based upon whether they had undertaken training or not also reveals those with training on the whole have a better understanding of terms. As illustrated in Table V, all security threats were better understood by those with training than those without – unfortunately, this also included the fake terms. Whilst the difference between those that had training and those that did not are not large (from 3%) for many of the terms, it is worth noting the large proportion of respondents in this survey who regard themselves as advanced users. It is therefore anticipated that this difference would be larger under normal circumstances. It is also noticeable that while the difference is small on well established threats such as virus, worms and spam; less

established threats such as Botnets and Zero-day attacks have a significantly larger difference between those with and without training.

TABLE VI. INFORMATION SECURITY PRACTICE OF RESPONDENTS

Good Security Practices	Respondents Who Received Training (%)	Respondents Who Did Not Receive Training (%)
I log off my computer whenever I leave a computer system	50	37
I backup my data on disks or CDs regularly	35	22
I check that antivirus software is enabled and updated	69	60
I use the organization's firewall protection	72	56
My passwords consists of at least 8 characters and uses the combination of letters (a-z), symbols (!@#%) and numbers (0-9)	72	45
I keep my password a secret and only I know it	84	61
I change my password regularly	23	9
I scan with antivirus any external disk/thumb drive/USB drive when first plugging it into the computer system	43	27
I report to security incidents to the appropriate parties	33	14
I look for "https://" or the "little gold padlock" before I make financial transaction online	60	54
I protect confidential files with passwords	36	23
I read the privacy statement before I proceed with an action (such as registering with a website, installing an application or financial/online banking transaction)	34	17
I ensure nobody is looking at my keyboard each time I key in my password	57	37

In terms of understanding how training effects actual practice, respondents were asked several questions about common security practices. Table VI illustrates the findings from these questions based upon whether they had undertaken training or not. More significantly from these results it is identifiable that a bigger difference exists in practice between those that had training and than those that did not. A good example here is the use of strong passwords for user authentication, with 72% of those trained using them but only 45% of those un-trained doing so. Training therefore is arguably having a positive effect not only upon awareness but also on actual practice. Unfortunately however, it is also evident that the level of practice amongst the trained respondents is not necessarily as high as would be liked with certain practices such as changing passwords and reporting incidents as low as 23 and 33% respectively.

In order to understand the effectiveness of users practice at home based upon whether they had received training, participants were asked a series of questions. Table VII illustrates that practice at home for those respondents with training is significantly better than those without – with practice differing from 7 to 17%. Similarly with the previous question, the level to which trained user's are actually following good practice is worryingly low, highlighting some potential concerns over the nature and type of training been undertaken.

TABLE VII. INFORMATION SECURITY PRACTICE AT HOME

Good Security Practices	Respondents Who Received Training (%)	Respondents Who Did Not Receive Training (%)
I shred confidential documents before throwing them into the bin	50	38
I change the default password for my router	53	36
I use encryption key to protect my wireless connection	58	51

Security controls are one of the first defense layers that protect users from security threats. The survey finally tried to understand what kind of security controls were used by respondents while at home. The results are shown in Table VIII. Even though respondents do not receive training, 97% of them are using Antivirus at home. This could be related with the results discussed in the previous section where 92% of them are aware of the virus/worm threats and take necessary action such as installing Antivirus. Overall, there is no significant difference between those who received training and those who did not. However, the results do demonstrate that those trained respondents are still marginally ahead of those who are not in using security controls at home.

TABLE VIII. RESPONDENTS' USE OF SECURITY CONTROLS

Security Controls	Respondents Who Received Training (%)	Respondents Who Did Not Receive Training (%)
Antivirus	98	97
Firewall	78	72
Anti-phishing	45	38
Anti-spyware	75	75
Intrusion Detection Systems (IDS)	20	18
Spam filter	67	66

Discussion

On the whole, the participants represented a well-informed group of individuals on the topic of Information Security, with respondents generally having a good level of awareness and practice. Care should therefore be given in generalizing these results to a wider population as it is anticipated that the levels of IT and security awareness would be generally lower. Whilst this does not affect the key results of the survey, it is important to realize that the problem of achieving information security

awareness and practice still remains. Indeed, even within this well educated demographic, 50% of them felt they had an average or lower level of awareness.

Whilst establishing the effectiveness of awareness training is not a simple task, the results have demonstrated that respondents whom have undertaken training are more aware of a greater variety of security issues – particularly threats. With the ever-changing security landscape and people's increasing adoption of technology, the need to maintain up-to-date levels of awareness is imperative if users are to remain secure. Indeed, the last few years alone has seen a significant increase in security threats that focus upon the human-factor, such as Phishing, that countermeasures were unable to protect against. Only through relevant and timely training can security be maintained.

Encouragingly, when looking at the motivations of participants in undertaking some form of education on information security, respondents appear very willing to engage to some degree both in home and workplace environments. Unfortunately, however, the volume and depth of such education is lacking in places – with only 36% of organizations willing to invest in security education and home users arguably lacking in credible, structured learning, given their focus upon web searches and news reports. What is evident from the findings is the participant's freedom of choice when looking to learn about security – both in terms of what they learn and how. Flexibility therefore appears to be an important consideration, so that users are able to learn what topics they want, in a manner or learning style they prefer, at a time and location they feel most comfortable in.

As motivation of home users will inevitable be problematic due to the various constraints of every-day life, focus therefore arguably has to be placed upon what can be achieved in the workplace. With 95% of participants who have training provided; attending, and home users stating that what they learn in the workplace is key to what they practice at home, leveraging workplace learning could potentially be very useful in establishing good security practice independent of the environment. The workplace environment is also better placed to ensure a credible and structured security awareness program is in place to ensure important aspects of knowledge are not missed. Industry therefore has an important role to play in educating employees on the subject of information security awareness; however, it is important to ensure such training is not too specifically focused upon any particular company's processes and is easily generalizable so that employees are able to apply such knowledge within the home environment.

CONCLUSIONS

Achieving good information security awareness in the general population of Internet users is imperative if they are to remain secure and electronic business is to thrive. Unfortunately, educating users about the threats and countermeasures in a dynamic environment like security requires time, resources and motivation. Comparing the home and work environments, it is clear the latter provides more opportunity for such education to take place – with companies motivated to provide training due to changes in legislation, regulation and governance. The survey findings have already demonstrated that leveraging this transference of knowledge from the workplace to home is already underway.

Whilst the workplace provides a good opportunity to educate users about information security, it has also become apparent that care

needs to be taken when looking into what they are taught, when they are taught it and how they like to learn. Given the mixture of differing priorities of business; cost; the varying degrees of prior knowledge of security from employees; and the differing pedagogies required, it follows that a highly flexible framework is required that is capable of tailoring information security awareness training to the individual across all environments: work and home. Future research will focus upon the developing such a framework and in particular look to incorporate other factors such as psychological profiling in order to maximize the learning experience but importantly also ensure that learning follows through to practice.

Acknowledgment

The authors would like to thank to Ministry of Higher Education Malaysia and the International Islamic University Malaysia for their funding of the scholarship for this research.

References

- [1] S. Hinde, "Hacking gains momentum," *Computer Fraud & Security*, vol. 2004, pp. 13-15, 2004.
- [2] R. Richardson, "2007 CSI computer crime and security survey," in *The 12th annual computer crime and security survey*: Computer Security Institute, 2007.
- [3] Harris Interactive, "Online security and privacy study," 2009.
- [4] B. Schneier, *Secrets and lies*. Indiana: Wiley Publishing, Inc., 2000.
- [5] R. Richardson, "2008 CSI computer crime & security survey," Computer Security Institute 2008.
- [6] BERR, "The 9th information security breaches survey," Department for Business Enterprise and Regulatory Reform & Pricewaterhouse Coopers, United Kingdom 2008.
- [7] Symantec, "Symantec Internet security threat report - Trends for January - June 2007," Symantec Corporation 2007.
- [8] GetSafeOnline, "Get safe online with free, expert advice." 2009.
- [9] StaySafeOnline, "Are your defenses up and your instincts honed?." 2009.
- [10] WebWise, "The BBC guide to using the Internet." 2009.
- [11] R. von Solms and S. H. von Solms, "Information security governance: Due care," *Computers & Security*, vol. 25, pp. 494-497, 2006.
- [12] M. T. Dlamini, J. H. P. Eloff, and M. M. Eloff, "Information security: The moving target," *Computers & Security*, vol. 28, pp. 189-198, 2009.
- [13] G. Rotvold, "How to Create a Security Culture in Your Organization," *Information Management Journal*, vol. 42, pp. 32-38, 11 2008.
- [14] S. Furnell and K.-L. Thomson, "From culture to disobedience: Recognising the varying user acceptance of IT security," *Computer Fraud & Security*, vol. 2009, pp. 5-10, 2009.
- [15] B. von Solms, "Information Security -- The Third Wave?," *Computers & Security*, vol. 19, pp. 615-620, 2000.
- [16] P. A. Chia, S. B. Maynard, and A. B. Ruighaver, "Understanding organizational security culture," in *Sixth Pacific Asia Conference on Information Systems Tokyo, Japan, 2002*, pp. 731-740.
- [17] T. Schlienger and S. Teufel, "Analyzing information security culture: Increased trust and appropriate information security culture," in *14 th International Workshop on Database and Expert Systems Applications, 2003 (DEXA'03) Prague, Czech Republic, 2003*.
- [18] McAfee, "McAfee security tips - 13 ways to protect your system." 2009.
- [19] Microsoft, "Consumer online safety education." 2009.
- [20] NCSA and Symantec, "NCSA-Symantec national cyber security awareness study newsworthy analysis," 2008.
- [21] C. C. Wood, "Information security awareness raising methods," *Computer Fraud & Security Bulletin*, vol. 1995, pp. 13-15, 1995.
- [22] P. Spurling, "Promoting security awareness and commitment," *Information Management & Computer Security*, vol. 3, pp. 20-26, 1995.
- [23] S. Hawkins, D. C. Yen, and D. C. Chou, "Awareness and challenges of Internet security," *Information Management & Computer Security*, vol. 8, pp. 131-143, 2000.
- [24] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," *Computers & Security*, vol. 26, pp. 63-72, 2007.
- [25] ENISA, "The new users' guide: How to raise information security awareness," European Network and Information Security Agency 2008.
- [26] M. E. Thompson and R. von Solms, "Information security awareness: Educating your users effectively," *Information Management & Computer Security*, vol. 6, pp. 167-173, 1998.
- [27] C. C. Chen, B. D. Medlin, and R. S. Shaw, "A cross-cultural investigation of situational information security awareness programs," *Information Management & Computer Security*, vol. 16, pp. 360-376, 2008.
- [28] E. Albrechtsen, "A qualitative study of users' view on information security," *Computers & Security*, vol. 26, pp. 276-289, 2007.
- [29] M. H. Cooper, "Information security training: lessons learned along the trail," in *Proceedings of the 36th annual ACM SIGUCCS conference on User services conference Portland, OR, USA: ACM, 2008*.
- [30] BBC, "Web networkers 'at risk of fraud'," 2007.
- [31] H. Wallop, "Fears over Facebook identity fraud," *Telegraph Media Group Limited*, 2007.
- [32] D. Adlam, "Social networking identity fraud," 2009.

Establishing a Personalized Information Security Culture

Shuhaili Talib*

*University of Plymouth, United Kingdom
International Islamic University Malaysia, Malaysia*

Nathan L. Clarke

*University of Plymouth, United Kingdom
Edith Cowan University, Australia*

Steven M. Furnell

*University of Plymouth, United Kingdom
Edith Cowan University, Australia*

ABSTRACT

It has long been understood that good security cannot be achieved through technical means alone and a solid understanding of the issues and how to protect yourself is required from users. Whilst many initiatives, programs and strategies have been proposed to improve the level of information security awareness, most have been directed at organizations, with a few national programs focused upon home users. Given people's use of technology is primarily focused upon those two areas: the workplace and home, this paper seeks to understand the knowledge and practice relationship between these environments. Through the survey that was developed, it was identified that the majority of the learning about information security occurred in the workplace, where clear motivations, such as legislation and regulation, existed. It was also found that user's were more than willing to engage with such awareness raising initiatives. From a comparison of practice between work and home environments, it was found that this knowledge and practice obtained at the workplace was transferred to the home environment. Given this positive transferability of knowledge and the willingness to learn about how to remain secure, an opportunity exists to move away from specific organizational awareness programs and to move towards awareness raising strategies that, whilst deployed in the organization, will develop an all-round individual security culture for users independent of the environment within which they are operating.

Keywords: information security; information security awareness; security culture; security management

INTRODUCTION

The volume and nature of information security threats has evolved, moving away from technical savvy hackers demonstrating their skill, to organized and well establish crackers that aim to receive substantial financial rewards for their efforts (Hinde, 2004). This has resulted in an increase in cybercrime activities and subsequent threats end-users find themselves the target of. For example, in the Computer Security Institute (CSI) survey report stated that 52% of organizations had encountered threats in 2007 (Richardson, 2007). Another survey conducted by Harris on behalf of Microsoft and the National Cyber Security Alliance (NCSA) found that 64% of respondents had encountered a Phishing email – a threat

rarely encountered 5 years ago (Harris Interactive, 2009). To safeguard users a range of security countermeasures exist. These tools continually evolve in sophistication and increase in number to counter the changing nature of the threats. However, in order for these to operate successfully they inherently rely upon the end-user to be able to deploy, configure and operate them. Unfortunately, it is also a well recognized fact that security is only as strong as the weakest link; and the weakest link is frequently the end-user (Schneier, 2000).

To counter the threat caused by end-users an increased focus has been given towards information security awareness and the need to educate and inform end-users. Within an organizational context, efforts towards improving awareness amongst employees have increased with CSI survey indicating 82% of Enterprise organizations having training programs (Richardson, 2008). Unfortunately, however, this is not necessarily the case for all, with Business Enterprise Regulatory Reform (BERR) Information Security Breach Survey, which largely comprises of small-to-medium sized companies (SMEs), indicating only 40% of their respondents conduct training (Business Enterprise Regulatory Reform, 2008). Whilst many organizations arguably have the resources to provide such training, should they deem it important to do so, they only represent a (95%) proportion of people who use the Internet. The remaining users are typically home-users or the general public. Worryingly, evidence demonstrate that it is this group of users that are most at risk, with 95% of all attacks being focused upon them (Symantec, 2007). Home users have a variety of resources at their disposal in order to improve their awareness of online threats. All the major Anti-Virus providers, Operating System vendors and government initiatives provide supporting information to the home user (GetSafeOnline, 2009; StaySafeOnline, 2009; WebWise, 2012).

Whilst training programs and initiatives exist within both the workplace and home, little research has been conducted to understand what is being taught and where, the effectiveness of such strategies and to what degree learning styles play a role in achieving good information security practice. Information security awareness can be tackled from a variety of different directions, such as within school, government-sponsored initiatives and security providers; however, this paper will specifically focus upon and investigate behavior, practices and interactions within and between organizations and home environments. The paper is organized as follows: Section II discusses the current state-of-art in information security awareness and the development of security culture. Section III describes the methodology of the study, with Section IV presenting the results. Section V discusses the main findings of the study with the conclusion and future work being presented in Section VI.

PRIOR WORK IN INFORMATION SECURITY AWARENESS TRAINING

Information security awareness has been given an increasingly important focus within both academic and commercial communities. Organizations are gradually understanding the importance of their information assets and developing strategies to improve awareness throughout the company. Good corporate governance, regulation and legislation have also helped in raising the importance and relevance of good information security policies and practices (von Solms and von Solms, 2006). Within academia, focus by researchers has partially moved away from the technical issues towards understanding the end user and developing models and programs that organizations can utilize in developing better awareness (Dlamini *et al.*, 2009).

Interestingly, within academia, current research is suggesting that simple awareness strategies that educate employees about particular security topics through traditional mechanisms such as class-room based teaching, online education and poster/email campaigns are not sufficient in maintaining long-term information security practice (Rotvold, 2008; Furnell and Thomson, 2009). Rather an increasing volume of research is proposing the need to develop an information security culture within the organization – moving away from surface learning and embedding or indoctrinating good practice within employees (von Solms, 2000; Chia *et al.*, 2002; Schlienger and Teufel, 2003; Furnell and Thomson, 2009). The authors of these studies believe through establishing an information security culture in the organization, long-term security practice can be maintained and moreover, the drive towards awareness and education of security issues becomes self-fulfilling, as employees are engaged and proactive about their practice.

Within the context of home users, awareness raising initiatives have been created. GetSafeOnline is a UK Government sponsored initiative that provides a blanket based approach; providing general information about the risks and how to get protected (GetSafeOnline, 2009). The site provides a variety of information from beginnings guides to specific information about relevant threats in a timely fashion. The site is predominately text based information with the addition of occasional video files. Other countries such as the USA have similar national based websites (StaySafeOnline, 2009). A number of companies that provide security software and operating systems also provide web-based access to resources – largely reading based – to assist in educating and informing home users (McAfee, 2009; Microsoft, 2009).

Arguably, motivating home users into undertaking security training is challenging as security is always a requirement but never actually the primary task the user is trying to achieve. People often do not have the understanding they need to do it and moreover for those that do, they frequently do not have the time or inclination in any case. Worryingly, evidence demonstrates even when users do think they know about security and how to protect themselves, this is often found not to be the case. A joint study by NCSA and Symantec found that while 75% of home users thought they had spam protection, in fact only 42% actually did (National Cyber Security Alliance and Symantec, 2008). This disparity between what they think they have and actually do have illustrates a significant gap in their understanding.

In order to achieve good security awareness considerable research has been undertaken into developing various learning mechanisms, such as: face-to-face training sessions, email messages, online training, video game, intranet-based access and poster campaigns (Spurling, 1995; Wood, 1995; Hawkins *et al.*, 2000; Cone *et al.*, 2007; European Network and Information Security Agency, 2008). Whilst focus has been given to what and how to educate within organizations, research has identified the importance of measuring the effectiveness of such programs in order to ensure education leads to practice (Thompson and Von Solms, 1998; Chen *et al.*, 2008). The CSI survey reported that 68% of the organizations measure the effectiveness of their awareness training (Richardson, 2008). Unfortunately, no figures were given as to the actual levels of effectiveness of the training. Various approaches have been identified to assist in creating an effective security program, such as, having more user engagement in the process through workshops and providing the training on a continuous basis. (Albrechtsen, 2007; Cooper, 2008; Dlamini *et al.*, 2009).

However, whilst such strategies might be possible for organizations to utilize, home users would find it arguably difficult to engage for a multitude of reasons: desire, time, resources and the knowledge they

need to, to name but a few. Unfortunately, there is little evidence demonstrating whether home users are in fact knowledgeable about information security and indeed practicing it.

A SURVEY OF END-USER AWARENESS AND PRACTICES

Given the prior literature in the area, it was concluded that it was difficult to determine the effectiveness of training and moreover where and how they received that training. In addition, whilst it could be hypothesized that the majority of training came from organizations, it is not clear exactly to what extent learning from work and home played a role in information security practice in general. A survey was therefore created to assess these factors. A quantitative method of collecting data was chosen for the study in order to maximize the number of respondents across a broad spectrum of industries and roles. The aims of the survey are:

- To understand respondents general levels of security awareness and practice.
- To understand whether they received training from work and if so, what type and how effective it was.
- To understand the relationship between knowledge gained and practice between work and home
- To understand how people learn and what preferences they have towards various learning styles.

The survey consists of four sections: Demographics; Information Security Awareness; Practice at Workplace and Practices at Home. The Practices at Workplace, sought to investigate the current practice of respondents at their workplace. The section also enquired about the type of training that they have attended and what the learning methods that they have experienced had been and what they preferred. Respondents were also asked about the sources of information security knowledge in the workplace. This section provided information about the degree of transferability of information security knowledge between home and the workplace. At the end of the section is a list of common security practices that have been created to understand what their practices at their workplace actually are. The final section on Practices at Home sought to mirror much of the composition of the previous section but with a view to practices and education at home.

The survey was distributed to a wide range of people regardless of location but with the condition that they were in employment and regularly use a computer at home and their workplace. The study was undertaken from 20th August – 7th October 2008 (49 days). The survey collection has been stopped when it reached more than the survey target (300) respondents. The survey was promoted via email, based on the authors' academic contacts, personal contacts, from the word-of-mouth and two mailing lists such as Google and Yahoo

groups. A total of 333 responses were obtained and the results are analyzed in the sections that follow.

RESULTS

An analysis of the demographics identified that a fairly even split in responses were received from both genders (55% male; 45% female). It was found that the majority of the respondents (55%) were from the age group 25 to 34 and 81% had at least an undergraduate level of education. This could be due to the personal contacts of the author and those who are in the age group are more likely to be IT literate and have at least an email account. Whilst this proportion of users are clearly not representative of the general population, it is not felt this would bias the results of the survey except to provide perhaps a more informed and educated response to the questions. The results therefore probably indicate a more positive perspective on the use and knowledge of information security than what exists within the general population.

Information Security Awareness

In order to assess the level of security awareness, respondents were asked to rate their perceived level against a five point scale. Almost half of them (49%) rated themselves at high or very high (as illustrated in Figure 1). When tied to the question asking respondents what their level of competency is with Information Technology (IT), where 64% stated that they had at least an advanced level of knowledge, it can be surmised that this group of respondents are well educate and informed about IT and Information Security in general.

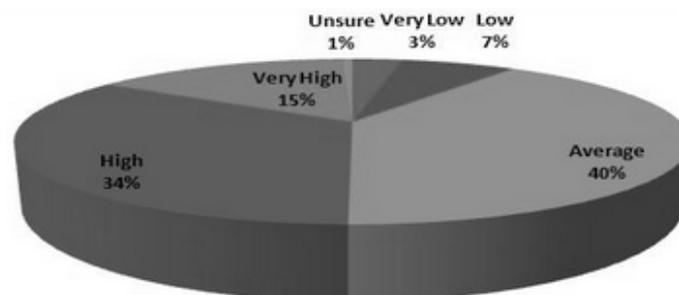


Figure 1. [Perceived level of information security awareness]

In order to better understand what aspects of information security respondents understood, they were asked a couple of questions surrounding their knowledge of security threats and their use of social networking sites. Table 1 presents the results of respondent's awareness of a variety of security threats. Un-surprisingly, the long-standing threats such as Virus and Spam were amongst the highest selected as being understood and newer threats such as zero-day attacks, Botnets ad Zombies less understood. Interestingly, whilst 70% understood Phishing, a relatively smaller 44% understood Social Engineering of which Phishing is an example of. The list of terms also included a couple of fake terms – Phlopping and Whooping – so that it was possible to identify respondents who might be exaggerating their knowledge or providing arbitrary responses. On the whole, relatively small numbers (7-10%) of

respondents thought they had heard and understood the terms. That said it is a little concerning that these terms received any acknowledgement at all.

Table 1. Perceived understanding of security threats

Information Security Terms	You Understand It (%)	You Never Heard Of It (%)
Virus/Worm	92	0
Trojan horse	80	3
Spam	90	0
Social engineering	44	24
Phishing	70	10
Pharming	24	42
Identity theft	81	8
Key loggers	57	22
Phlopping ^a	7	68
Botnets	33	43
Zombies	33	38
Denial of service	56	24
Packet sniffer	47	37
Whooping ^a	10	59
Hacker	95	1
Zero day attacks	29	44
Cracker	56	24
a. Fake security term		

Social networking is a popular Internet activity, which literature has suggested is a common threat vector when looking to obtain information about people for subsequent use in identity fraud (British Broadcasting Corporation, 2007; Wallop, 2007; Adlam, 2009). Amongst the respondents, 63% indicated they belong to one or more sites. When asked what information they release onto the social network, the respondent group overall appear to be informed and careful about releasing too much information. Table 2 illustrates that whilst 59% and 62% are releasing information regarding their real name and email address; only 7% reveal their full postal address. The most worrying statistic is the 45% releasing their date of birth but along with their name this amount of information is unlikely to result in identity theft.

Table 2. Personal information revealed by social networking.

Personal Information	Respondents (%)
Real name	59
Email	62
Real date of birth	45
Full address	8
Phone number	14
Personal blog	22
Special occasions	22
Photographs of yourself	67
Photographs of your family members	37
Photographs of your friends	42
Photographs of your office	7
Photographs of your house	8
None of the above	5
Other	1

Information Security Practices at Workplace

Analysing the participant's responses with reference to their practices within work, 36% stated their organization provided some sort of training with regards to information security. When comparing this to the size of the organization the respondent works for, it was found that 36% came from SMEs and coincidentally 36% also came from Enterprise (an Enterprise being defined as those organizations with 250 or greater employees). Whilst this figure is in line with the 40% stated by BERR survey, which largely canvases SMEs, it falls somewhat short of CSI Computer Crime and Security Survey's 80% (whose respondents are largely but not exclusively Enterprises)(Business Enterprise Regulatory Reform, 2008; Richardson, 2008). A further analysis of those responding on behalf of Enterprises shows that relatively few (3%) come from US-based companies – where regulation and legislation have arguably been prime motivators in ensuring staff are appropriately trained. Of the 36% of respondents who stated their organization provided training, 95% also stated they attended the training sessions.

In order to understand more about security practices in the workplace, respondents were asked about the sources of their information security knowledge. The top three information security sources at work are presented in Table 3; with websites and search engines the most popular. Arguably this could be due to many organizations now providing open access to the Internet. This freedom permits the employee to search and locate information of value at the time required. In addition to asking what their top three

sources of information security knowledge were, they were also asked what they prefer. Interestingly, the results from these two questions came out identically, illustrating user’s already have the freedom of choice when it comes to learning about information security and organizations are not burdening them with approaches they would not prefer.

From Table 3, it is evident that much of the knowledge for Information Security within a workplace comes from fairly informal means – web searches and informal discussions with colleagues. Interestingly, these results do illustrate the importance and relevant of the organizational policy in informing employees and moreover practice.

Table 3. Top three sources of information security & learning at work.

Top Three For Information Security In The Workplace		Top Three Most Preferred Sources For Information Security In The Workplace	
1	Websites and search engines	1	Websites and search engines
2	Informal discussions with colleagues and professional contacts	2	Information discussions with colleagues and professional contacts
3	Organization’s policy	3	Organization’s policy

This freedom of choice of how to learn comes through again when the respondents were asked about where or how they received their training. 28% of respondents responded that it was through self-study. As illustrated in Figure 2, the remaining options received a fairly even split, indicating that if organizations are willing to invest in training their staff, the methods utilized will vary with no single option being a considered standard. Interestingly, further analysis of these responds when taking into account the size of the organization found that the preferred training type was independent of the organizational size, with SMEs willing to invest in outside experts as much as Enterprises – countering the standard assumption that SMEs do not have the resources to pay for training and would rely upon less expensive options such as self-study or online training.

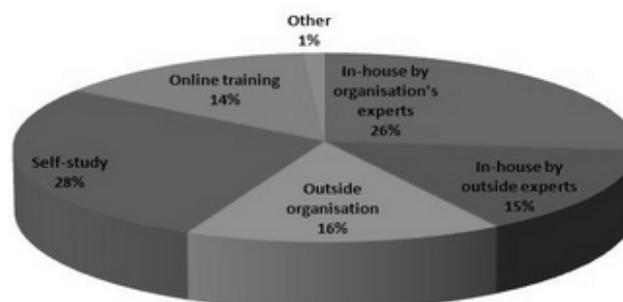


Figure 2. [Preferred training type]

Respondents were also asked how frequent they would like to have security training. As Figure 3 illustrates, the largest proportion of users preferred to have an on-demand service, with the majority of the remaining respondents split between monthly, quarterly, half-yearly and yearly. Overall 95% of respondents felt they needed some level of training.

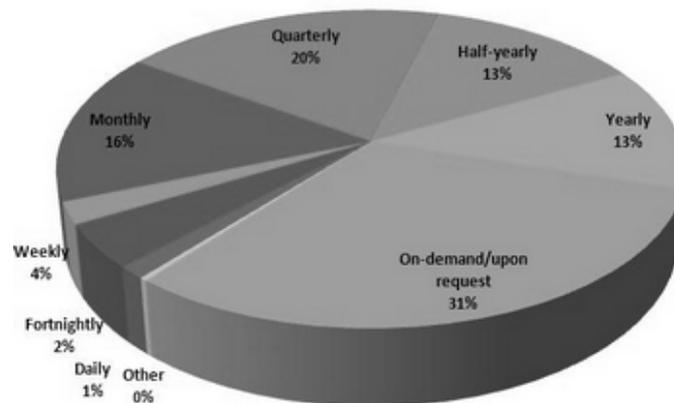


Figure 3. [Respondent preference to having information security training].

Information Security Practices at Home

In order to compare practice from the workplace and home, respondents were asked a series of questions with respect to their practice at home. When analysing the top three sources of acquiring information security knowledge and what sources they preferred to learn from, it can be seen that the lists were identical, with web searches coming out first, what they had learnt from the workplace second, and reading newspapers and magazines third (as illustrated in Table 4). Upon reflection, this correlation should be expected as within the home environment you have complete freedom over what and how you learn. The user is not forced through employment to attend training courses or learn in a specific manner depending upon how the organization has decided to implement training. This freedom provides the user with the opportunity of using learning approaches that are preferred and most convenient to the individual. Arguably, without the formal training approaches that organizations utilize it is difficult to understand the depth of learning that goes on at home – with much of the learning likely being a result of news articles and press coverage of a particular event. A further research that focused on the level of understanding of information security knowledge acquired at home would be required to further explore on this aspect.

That said, the results from Table 4 do illustrate the users are willing and do learn at home. Interestingly, the second most preferred source of information is what they learn from the workplace. Acquiring knowledge about information security within the workplace has an impact upon the level of awareness and learning at home.

Table 4. Top three sources of information security & learning at home.

Top Three For Information Security At Home		Top Three Most Preferred Sources For Information Security At Home	
1	Websites and search engines	1	Websites and search engines
2	From what I learnt at my workplace	2	From what I learnt at my workplace
3	Daily newspaper and Magazines	3	Daily newspaper

In addition to understanding how they learn, respondents were also asked how frequent that learning takes place. Figure 4 presents the breakdown of responses. 71% of respondents undertake some level of training at home with 39% performing this on average on a monthly basis and 25% weekly. Whilst the regularity of the training is somewhat infrequent, given the lack of motivation within the home environment to undertake training, it is encouraging to note that over two thirds are willing to undertake some level of training at home.

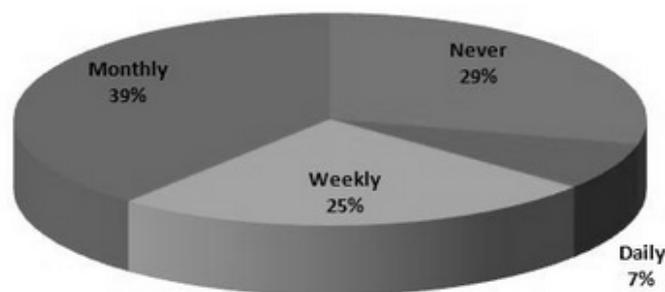


Figure 4. [How frequent learning takes place at home].

Given that the proportion of users not willing to learn at home and the proportion that learn on a monthly basis make up 68% of the respondents, the need to acquire the knowledge necessary to ensure they remain secure at home is imperative. Arguably therefore, the knowledge users obtain within the workplace and subsequently transfer into the home environment is key to establishing a level of

information security awareness for many respondents. Without such transference, a good proportion of home users will have little or no security awareness.

Effectiveness of Information Security Training

Having established training practices at home and the workplace, the survey proceeded to understand the extent to which this training and practice was effective. A total of 115 of the total respondents received training, 115 did not and the remaining claimed that they are not sure they have attended the training. Whilst training, awareness and practice are arguably associated with each other, simply undertaking training or having an awareness of an issue does not necessarily imply practice.

To this end, Figure 5 provides a comparison between those respondents who undertook training and what they considered their level of security awareness is. A total of 67% of respondents who undertook training felt they had a high or very high level of awareness. This compares to just 43% who had not received training. This demonstrates respondents at least perceive they have a better understanding of the information security threats and countermeasures over those that have not received training.

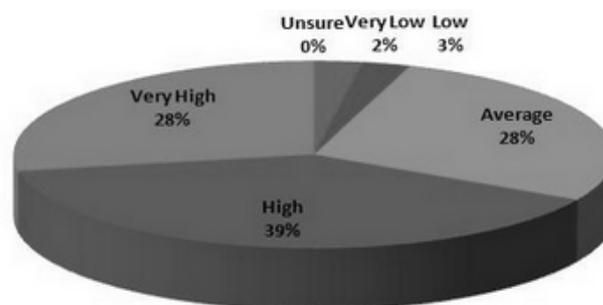


Figure 5. [Respondents who attended training and their awareness level].

A further analysis of respondents' understanding of various security threats based upon whether they had undertaken training or not also reveals those with training on the whole have a better understanding of terms. As illustrated in Table 5, all security threats were better understood by those with training than those without – unfortunately, this also included the fake terms. Whilst the difference between those that had training and those that did not are not large (from 3%) for many of the terms, it is worth noting the large proportion of respondents in this survey who regard themselves as advanced users. It is therefore anticipated that this difference would be larger under normal circumstances. It is also noticeable that while the difference is small on well established threats such as virus, worms and spam; less established threats such as Botnets and Zero-day attacks have a significantly larger difference between those with and without training.

Table 5. Perceived understanding of security threats based upon whether training had been provided.

Information Security Terms	Respondents Who Received Training (%)	Respondents Who Did Not Receive Training (%)
Virus/Worm	97	93
Trojan horse	94	77
Spam	94	88
Social engineering	58	40
Phishing	81	67
Pharming	34	20
Identity theft	85	81
Key loggers	72	55
Phlopping ^a	10	5
Botnets	50	28
Zombies	50	30
Denial of service	75	56
Packet sniffer	65	48
Whooping ^a	17	8
Hacker	97	95
Zero day attacks	45	23
Cracker	73	55
a. Fake security term		

In terms of understanding how training effects actual practice, respondents were asked several questions about common security practices. Table 6 illustrates the findings from these questions based upon whether they had undertaken training or not. More significantly from these results it is identifiable that a bigger difference exists in practice between those that had training and than those that did not. A good example here is the use of strong passwords for user authentication, with 72% of those trained using them but only 45% of those un-trained doing so. Training therefore is arguably having a positive effect not only upon awareness but also on actual practice. Unfortunately however, it is also evident that the level of practice amongst the trained respondents is not necessarily as high as would be liked with certain practices such as changing passwords and reporting incidents as low as 23 and 33% respectively.

Table 6. Information security practice of respondents.

Good Security Practices	Respondents Who Received Training (%)	Respondents Who Did Not Receive Training (%)
I log off my computer whenever I leave a computer system	50	37
I backup my data on disks or CDs regularly	35	22
I check that antivirus software is enabled and updated	69	60
I use the organization's firewall protection	72	56
My passwords consists of at least 8 characters and uses the combination of letters (a-z), symbols (!@#\$%) and numbers (0-9)	72	45
I keep my password a secret and only I know it	84	61
I change my password regularly	23	9
I scan with antivirus any external disk/thumb drive/USB drive when first plugging it into the computer system	43	27
I report to security incidents to the appropriate parties	33	14
I look for "https://" or the "little gold padlock" before I make financial transaction online	60	54
I protect confidential files with passwords	36	23
I read the privacy statement before I proceed with an action (such as registering with a website, installing an application or financial/online banking transaction)	34	17
I ensure nobody is looking at my keyboard each time I key in my password	57	37

In order to understand the effectiveness of users practice at home based upon whether they had received training, participants were asked a series of questions. Table 7 illustrates that practice at home for those respondents with training is significantly better than those without – with practice differing from 7 to 17%. Similarly with the previous question, the level to which trained user's are actually following good practice is worryingly low, highlighting some potential concerns over the nature and type of training been undertaken.

Table 7. Information security practice at home.

Good Security Practices	Respondents Who Received Training (%)	Respondents Who Did Not Receive Training (%)
I shred confidential documents before throwing them into the bin	50	38
I change the default password for my router	53	36
I use encryption key to protect my wireless connection	58	51

Security controls are one of the first defense layers that protect users from security threats. The survey finally tried to understand what kind of security controls were used by respondents while at home. The results are shown in Table 8. Even though respondents do not receive training, 97% of them are using Antivirus at home. This could be related with the results discussed in the previous section where 92% of them are aware of the virus/worm threats and take necessary action such as installing Antivirus. Overall, there is no significant difference between those who received training and those who did not. However, the results do demonstrate that those trained respondents are still marginally ahead of those who are not in using security controls at home.

Table 8. Respondents' use of security controls.

Security Controls	Respondents Who Received Training (%)	Respondents Who Did Not Receive Training (%)
Antivirus	98	97
Firewall	78	72
Anti-phishing	45	38
Anti-spyware	75	75
Intrusion Detection Systems (IDS)	20	18
Spam filter	67	66

DISCUSSION

On the whole, the participants represented a well-informed group of individuals on the topic of Information Security, with respondents generally having a good level of awareness and practice. Care should therefore be given in generalizing these results to a wider population as it is anticipated that the levels of IT and security awareness would be generally lower. Whilst this does not affect the key results of the survey, it is important to realize that the problem of achieving information security awareness and

practice still remains. Indeed, even within this well educated demographic, 50% of them felt they had an average or lower level of awareness.

Whilst establishing the effectiveness of awareness training is not a simple task, the results have demonstrated that respondents whom have undertaken training are more aware of a greater variety of security issues – particularly threats. With the ever-changing security landscape and people’s increasing adoption of technology, the need to maintain up-to-date levels of awareness is imperative if users are to remain secure. Indeed, the last few years alone has seen a significant increase in security threats that focus upon the human-factor, such as Phishing, that countermeasures were unable to protect against. Only through relevant and timely training can security be maintained.

Encouragingly, when looking at the motivations of participants in undertaking some form of education on information security, respondents appear very willing to engage to some degree both in home and workplace environments. Unfortunately, however, the volume and depth of such education is lacking in places – with only 36% of organizations willing to invest in security education and home users arguably lacking in credible, structured learning, given their focus upon web searches and news reports. What is evident from the findings is the participant’s freedom of choice when looking to learn about security – both in terms of what they learn and how. Flexibility therefore appears to be an important consideration, so that users are able to learn what topics they want, in a manner or learning style they prefer, at a time and location they feel most comfortable in.

As motivation of home users will inevitable be problematic due to the various constraints of every-day life, focus therefore arguably has to be placed upon what can be achieved in the workplace. With 95% of participants who have training provided; attending, and home users stating that what they learn in the workplace is key to what they practice at home, leveraging workplace learning could potentially be very useful in establishing good security practice independent of the environment. The workplace environment is also better placed to ensure a credible and structured security awareness program is in place to ensure important aspects of knowledge are not missed. Industry therefore has an important role to play in educating employees on the subject of information security awareness; however, it is important to ensure such training is not too specifically focused upon any particular company’s processes and is easily generalizable so that employees are able to apply such knowledge within the home environment.

A Personalized Security Awareness Framework

Current approaches to information security awareness are obviously not fit for purpose. Whilst they are certainly better than nothing, they fail in providing the necessary learning for users to become and remain competent. The approach taken thus far by industry and research has focused on what to teach rather than how to, with the effect of awareness strategies that are “one size fits all”. This approach left users disappointed as they acquired little new knowledge (Okenyi and Owens, 2007). Studies have also

commented on how security awareness training is analogous to fitting a square peg in a round hole (Schultz, 2004).

Within school education it has been long understood that putting the learner at the centre of the learning experience is imperative for effective education. One core concept coming out from this approach is the idea of an individualized or personalized learning plan (Dainton, 2004; Burton, 2007; The National Strategies, 2007; Underwood and Banyard, 2008; Department for Children School and Families, 2010). Personalized learning has been defined as teaching based upon students' need or in other words it is tailor-made into the individuals interests and preferences (Dainton, 2004; Maguire, 2008). Personalized learning also provides the opportunity of understanding how an individual learns, adopting different learning strategies to maximize the effectiveness of education (Sternberg *et al.*, 2008). Personalization of learning also enables learners to set their own learning objectives which provide flexibility in the learning process itself (Campbell *et al.*, 2007). Whilst prior literatures suggesting individualized learning can improve learning outcomes; little research has been undertaken in the field of information security education (Brocke and Buddendick, 2005; May, 2008).

When considering the factors or attributes that affect learning, a myriad of internal, external, direct and indirect aspects arise. Figure 6 below illustrates a mind-map of factors that need to be considered if a flexible, individual and robust framework for information security awareness education is to be developed.

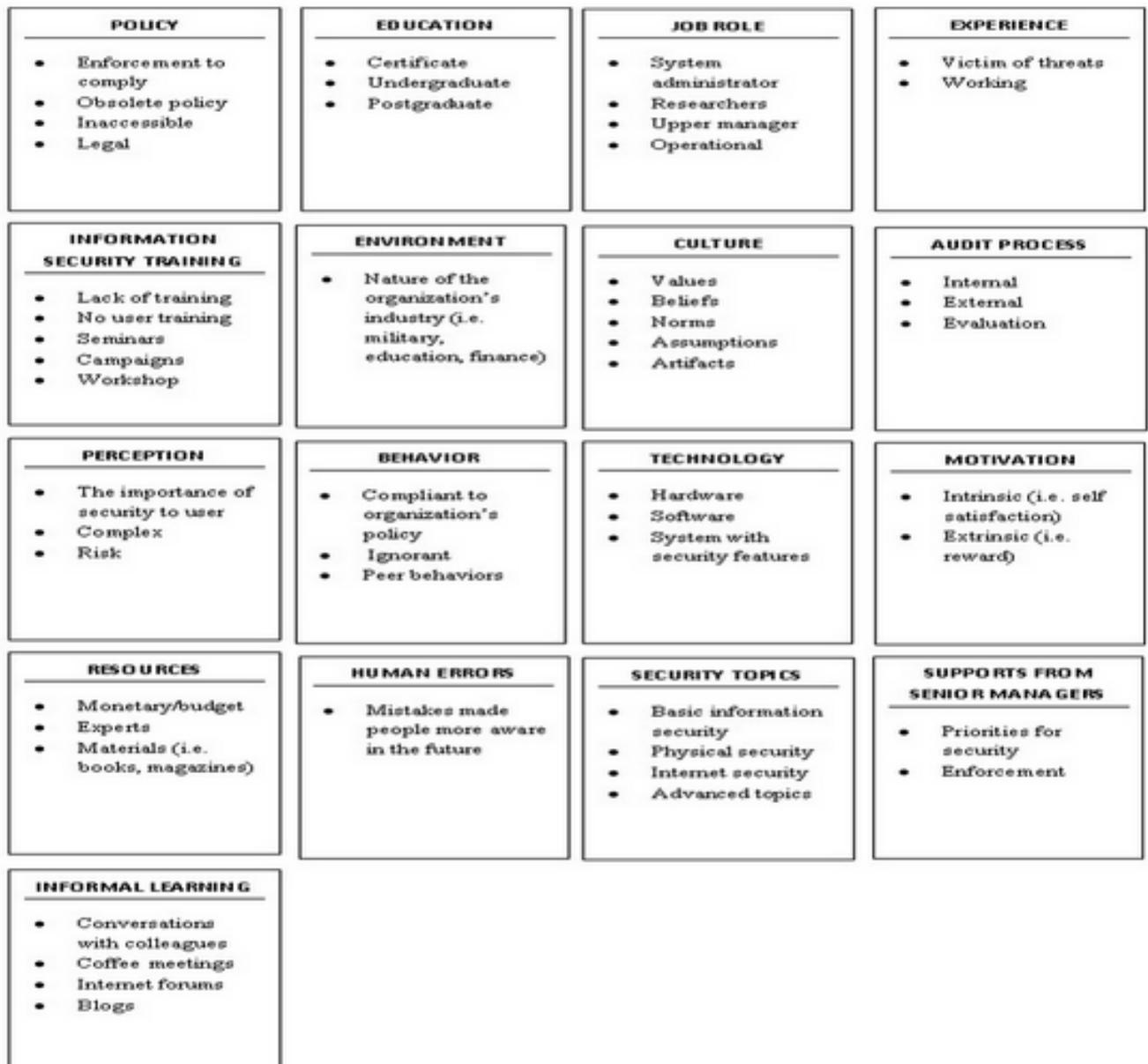


Figure 6. [Factors affecting information security awareness].

CONCLUSION

Achieving good information security awareness in the general population of Internet users is imperative if they are to remain secure and electronic business is to thrive. Unfortunately, educating users about the threats and countermeasures in a dynamic environment like security requires time, resources and motivation. Comparing the home and work environments, it is clear the latter provides more opportunity

for such education to take place – with companies motivated to provide training due to changes in legislation, regulation and governance. The survey findings have already demonstrated that leveraging this transference of knowledge from the workplace to home is already underway.

Whilst the workplace provides a good opportunity to educate users about information security, it has also become apparent that care needs to be taken when looking into what they are taught, when they are taught it and how they like to learn. Given the mixture of: differing priorities of business; cost; the varying degrees of prior knowledge of security from employees; and the differing pedagogies required, it follows that a highly flexible framework is required that is capable of tailoring information security awareness training to the individual across all environments: work and home. Future research will focus upon the developing such a framework and in particular look to incorporate other factors such as psychological profiling in order to maximize the learning experience but importantly also ensure that learning follows through to practice.

REFERENCES

- Adlam, D. (2009). Social networking identity fraud. Retrieved 2 September 2009, from <http://ezinearticles.com/?Social-Networking-Identity-Fraud&id=2730177>
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276-289.
- British Broadcasting Corporation (2007). Web networkers 'at risk of fraud'. Retrieved 2 September 2009, from <http://news.bbc.co.uk/1/hi/uk/6910826.stm>
- Brocke, J. v., & Buddendick, C. (2005). Security awareness management - Foundations and Implementation of security awareness. Paper presented at the 2005 International Conference on Security and Management (SAM'05), Las Vegas, USA.
- Burton, D. (2007). Psycho-pedagogy and personalised learning. *Journal of Education for Teaching: International research and pedagogy*, 33(1), 5 - 17.
- Business Enterprise Regulatory Reform (2008). The 9th information security breaches survey. United Kingdom: Department for Business Enterprise and Regulatory Reform & Pricewaterhouse Coopers.
- Campbell, R. J., Robinson, W., Neelands, J., Hewston, R., & Mazzoli, L. (2007). Personalised learning: Ambiguities in theory and practice. *British Journal of Educational Studies*, 55(2), 135-154.
- Chen, C. C., Medlin, B. D., & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security*, 16(4), 360-376.
- Chia, P. A., Maynard, S. B., & Ruighaver, A. B. (2002). Understanding organizational security culture. Paper presented at the Sixth Pacific Asia Conference on Information Systems Tokyo, Japan.

- 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.
- Cooper, M. H. (2008). Information security training: lessons learned along the trail. Paper presented at the Proceedings of the 36th annual ACM SIGUCCS conference on User services conference.
- Dainton, S. (2004). Personalised learning. *Symposium Journals 2004* 46(2), 56-58.
- Department for Children School and Families (2010). Personalised learning approaches used by schools Retrieved 6 May 2010, from <http://www.dcsf.gov.uk/research/programmeofresearch/projectinformation.cfm?projectId=14664&type=5&resultspage>
- Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, 28(3-4), 189-198.
- European Network and Information Security Agency (2008). The new users' guide: How to raise information security awareness: European Network and Information Security Agency.
- 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.
- GetSafeOnline (2009). Get safe online with free, expert advice. Retrieved 23 July 2009, from <http://www.getsafeonline.org/>
- Harris Interactive (2009). Online security and privacy study. Retrieved 23 July 2009, from <http://staysafeonline.mediaroom.com/index.php?s=67>
- Hawkins, S., Yen, D. C., & Chou, D. C. (2000). Awareness and challenges of Internet security. *Information Management & Computer Security*, 8(3), 131-143.
- Hinde, S. (2004). Hacking gains momentum. *Computer Fraud & Security*, 2004(11), 13-15.
- Maguire, A. (2008). Achieving real personalised learning: Considerations on blended learning Retrieved 30 March 2010, from http://www.thirdforce.com/resources/whitepaper/WP_AMaguire01.pdf
- May, C. (2008). Approaches to user education. *Network Security*, 2008(9), 15-17.
- McAfee (2009). McAfee security tips - 13 ways to protect your system Retrieved 2 September 2009, from http://www.mcafee.com/us/threat_center/tips.html
- Microsoft (2009). Consumer online safety education Retrieved 2 September 2009, from <http://www.microsoft.com/protect/default.aspx>

- National Cyber Security Alliance, & Symantec (2008). NCSA-Symantec national cyber security awareness study newsworthy analysis.
- Okenyi, P. O., & Owens, T. J. (2007). On the Anatomy of Human Hacking. [Article]. *Information Systems Security*, 16, 302-314.
- Richardson, R. (2007). 2007 CSI computer crime and security survey. The 12th annual computer crime and security survey. Retrieved 22 August 2008, from <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf>
- Richardson, R. (2008). 2008 CSI computer crime & security survey: Computer Security Institute.
- Rotvold, G. (2008). How to Create a Security Culture in Your Organization. *Information Management Journal*, 42(6), 32-38.
- Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: Increased trust and appropriate information security culture. Paper presented at the 14 th International Workshop on Database and Expert Systems Applications, 2003 (DEXA'03) Prague, Czech Republic.
- Schneier, B. (2000). *Secrets and lies*. Indiana: Wiley Publishing, Inc.
- Schultz, E. (2004). Security training and awareness--fitting a square peg in a round hole. *Computers & Security*, 23(1), 1-2.
- Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security*, 3(2), 20-26.
- StaySafeOnline (2009). Are your defenses up and your instincts honed? Retrieved 23 July 2009, from <http://www.staysafeonline.org/>
- Sternberg, R. J., Grigorenko, E. L., & Zhang, L.-f. (2008). Styles of learning and thinking matter in instruction and assessment. *Perspectives on Psychological Science*, 3(6), 486-506.
- Symantec (2007). Symantec Internet security threat report - Trends for January - June 2007: Symantec Corporation.
- The National Strategies (2007). Leading on intervention: Personalisation questions and answers Retrieved 30 March 2010, from <http://nationalstrategies.standards.dcsf.gov.uk/downloader/9e2a483e7a1c9191f017c6ddfe2dfc30.pdf>
- Thompson, M. E., & Von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, 6(4), 167-173.
- Underwood, J., & Banyard, P. (2008). Managers', teachers' and learners' perceptions of personalised learning: evidence from Impact 2007. *Technology, Pedagogy and Education*, 17(3), 233 - 246.
- von Solms, B. (2000). Information Security -- The Third Wave? *Computers & Security*, 19(7), 615-620.

von Solms, R., & von Solms, S. H. (2006). Information security governance: Due care. *Computers & Security*, 25(7), 494-497.

Wallop, H. (2007). Fears over Facebook identity fraud. Retrieved 2 September 2009, from <http://www.telegraph.co.uk/news/uknews/1556322/Fears-over-Facebook-identity-fraud.html>

WebWise (2009). The BBC guide to using the Internet. Retrieved 23 July 2009, from <http://www.webwise.com/>

Wood, C. C. (1995). Information security awareness raising methods. *Computer Fraud & Security Bulletin*, 1995(6), 13-15.