INFORMATION SECURITY BEHAVIOUR AMONG INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA STUDENTS

BY

FATEEMA LAMBENSA

A dissertation submitted in partial fulfilment of the requirements for the degree of Master of Information Technology

Kulliyyah of Information and Communication Technology
International Islamic University
Malaysia

APRIL 2010

ABSTRACT

The potential risks of using Internet have gradually increased as witnessed by the increasing number of security breach incidents from the critical issues of information security and privacy. Students regularly access to the Internet not only for completing their academic tasks but also for their personal purposes. Therefore, information and computer security are becoming the important issues. Effective privacy management and information security require a great understanding both technological and human dimensions. Thus, the purpose of this research is to investigate the university student’s behaviour towards information security and to examine factors influencing information security behaviour. The study is adopted the quantitative approach by conducting a survey among IIUM students having either personal computer or laptop. The questionnaires were distributed to the targeted respondents. Then, the SPSS software was used to systematically analyze all data obtained from the respondents and to generate statistical information and detailed analyses of the survey results. This study also explores the insights of information security behaviour. Hopefully, this study is contributed to an understanding of the influencing factors towards the university students’ behaviour in relation to information security. This would lead to organize more information security awareness programmes as the success of computer and information security greatly depends on the effective individual behaviours.

ملخّص البحث

المخاطر المحتملة لاستخدام شبكة الإنترنت قد زادت تدريجيّاً كما يشهد على ذلك العدد المتزايد من حوادث الخرق ال أمني الناتج في القضايا الحساسة التي تهم أمن المعلومات والخصوصية. عادةً، الطلاب لا يستخدمون الإنترنت لاستكمال برامجهم الأكاديمية فقط، ولكن أيضاً لخدمة أغراضهم الشخصية. بانتشار استخدام الإنترنت، على أي حال، أمن المعلومات والكمبيوتر أصبحت من القضايا الهامة. الخصوصية وفعالة لإدارة أمن المعلومات تتطلب تفهماً كبيراً سواء التكنولوجي والبعد الإنساني. ولذلك، فإن الغرض من هذا البحث هو دراسة الطالب الجامعي في السلوك تجاه أمن المعلومات ودراسة العوامل المؤثرة في سلوك أمن المعلومات. الدراسة استخدمت منهج كمي عن طريق إجراء دراسة استقصائية في أوساط طلاب الجامعة الإسلامية العالمية ماليزيا (IIUM) الذين يمتلكون حاسوب شخصي أو محمول. الاستبانات التي تم توزيعها عشوائياً، وتدار على المشاركين، تم البرتامج الإحصائي للعلوم الاجتماعية إيس.في.إيس.إيس (SPSS) المستخدمة لمنهجية تحليل جميع البيانات التي تم الحصول عليها من المجيبين وتوليد المعلومات الإحصائية. وهذه الدراسة قد تم اكتشافها من رؤية ثاقبة وأمن المعلومات السلوك. نتيجة هذه الدراسة يؤمل أن تسهم في تطوير وفهم العوامل العامة التي تؤثر على سلوك الطلاب الجامعيين نحو أمن المعلومات، وبالتالي قد تؤدي إلى مزيد من المعلومات الأمنية وتنظيم برامج للتوعية الأمنية ونجاح الأمن يعتمد أيضاً على السلوك الفعلي للأفراد.

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion, it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Information Technology.

……………………………..……..
Ramlah Hussein
Supervisor

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Information Technology.

....
Murni Mahmud
Examiner

This dissertation was submitted to the Department of Information Systems and is accepted as a partial fulfilment of the requirements for the degree of Master of Information Technology.

....
Abu Osman Md Tap
Head, Department of Information Systems

This dissertation was submitted to the Kulliyyah of Information and Communication Technology and is accepted as a partial fulfilment of the requirements for the degree of Master of Information Technology.

....
Mohd. Adam Suhaimi
Dean, Kulliyyah of Information and Communication Technology

DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Fateema Lambensa

Signature ……………………………………   Date……………………..…..

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

INFORMATION SECURITY BEHAVIOUR AMONG INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below.

1. Any material contained in or derived from this unpublished research may only be used by others in their writing with due acknowledgement.

2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.

3. The IIUM library will have the right to make, store in a retrieval system and supply copies of this unpublished research if requested by other universities and research libraries.

Affirmed by Fateema Lambensa.

……………………………........... ……..……..…………..

Signature Date

Dedication to:

My beloved parents, my dearest siblings, my beloved relatives and my best friends
Thank you from the bottom of my heart
For their love, prayers, encouragement, perseverance and faith in me

ACKNOWLEDGEMENTS

In the name of Allah, Most Gracious, Most Merciful.

Alhamdulillah, I am eternally grateful to Almighty God for His mercy, guidance and every blessing in my life, for without Him, none of this would be possible. *Salawat* and *Salam* are upon the Prophet Muhammad (S.A.W.), his family as well as his companions.

First of all, I would like to take this opportunity to express my gratitude to my supervisor, Assistant Professor Dr. Ramlah Hussein, for her advice, guidance, supervision and idea throughout the study. Her patience, kindness and understanding have helped me in completing the dissertation. Appreciation is also expressed to Assistant Professor Dr. Murni Mahmud for her criticism and valuable advice.

I would also like to thank all lecturers, staff and faculty members at Department of Information Systems as well as Centre for IT Advancement for their great support throughout this dissertation period.

Enormous thanks goes to my beloved family and relatives who constantly give many forms of support and encouragement during the difficult times. Thanks for their strong belief in my potential. They have been powerful source of my inspiration in studying and completing this dissertation.

My utmost thanks go to my dear friends; Toiyibah, Saini, Jannah, Mashita, Zakiah, Nojeem, who had constantly kept reminding and encouraging me to finish my dissertation within the time given.

I am also grateful to my sponsor for giving me support to pursue this Master of Information Technology programme.

Last but certainly not least, I would like to take this opportunity to thank all who have contributed to invaluable encouragement and guidance in my work at all stages and made it possible for me to complete this dissertation. May Allah (S.W.T.) reward all of them for their contribution and forgive me for all errors and shortcomings.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 INTRODUCTION

The rapid growth in computing and networking technologies has evolved in every aspects of our life. People rely on computers for everyday tasks more than ever for their personal, educational and business purposes. Changes in information and communication technology (ICT) and particularly their confluence have raised a number of concerns connected with the protection of organizational information assets (Dhillon & Backhouse, 2000).

Today, organizations' information assets are largely in electronic form. This electronic information is processed with the help of information systems, which communicate extensively over private networks and the Internet. The high level of connectivity, the availability of sophisticated hacking tools, the enormous growth of electronic commerce, and other factors have created unprecedented opportunities for the dark side of the technological advancement to emerge and prosper (Hu et al., 2007).

Attacks by computer viruses and spyware, and security breaches in computer systems are almost daily occurrences. Keeping computers secured is becoming increasingly difficult. Broucek and Turner (2003) mentioned that "in the age of hacktivism, malware and cyber-warfare, increasing number of publications are being produced by computer security specialists and systems administrators on technical issues arising from illegal or inappropriate on-line behaviours".

These incidents have serious effects on the economy and society including academia. A recent report, "Breaches in the Academia Sector", by John Correlli of JMC Privacy Consulting Group, noted that from 2005 through 2007, there were 277 widely reported breaches at colleges and universities in the United States. Furthermore, the 263 reported privacy data breaches in the United States in 2008, about one-third (76) occurred at colleges and universities (Claburn, 2009).

These breaches consequently led to gaining access to student’s personal information such as names, social security number, photos, grades, and other information, as well as current and former faculty and staff (Anderson, 2006; Ciampa, 2007). Effective privacy management and information security needs a great understanding both technical and human dimensions. This study seeks to understand what factors influence student’s behaviour towards information security.

1.2 BACKGROUND OF STUDY

The term information security describes the tasks of guarding information that is in a digital format typically manipulated by a microprocessor (like on personal computer), stored on a magnetic or optical storage device (like a hard drive or DVD), and is transmitted over a network (such as a local area network or the Internet) (Ciampa, 2007).

Information security is intended to protect information that has a high value to people and organizations to prevent data theft. Information security involves any process, activity, or task that protects the confidentiality, integrity, and availability of information (National Institute of Standards and Technology [NIST], 1995; Parker, 1998; Tudor, 2001).

For common computer and Internet users, information security may mean being able to work with computers without being attacked by viruses, being able to conduct on-line business without worrying that their credit card numbers will be stolen, being able to read e-mails without receiving spam, or being able to have a chat with friends without worrying that the information will be wiretapped (Huang et al., 2008).

Security of computers has become an issue of primary importance as the number and types of information security attacks gradually occur as witnessed by the increasing number of security breach incidents such as spread of computer viruses, and hackers' invasion of proprietary network sites. With more than one billion people connected to the Internet worldwide, it has had a revolutionary impact on how people learn, interact, and communicate (Ciampa, 2007).

Recent advance in computer technology and the diffusion of personal computers, software, multimedia, and network resources indicated the development and implementation of new and innovative teaching strategies (Sam et al, 2005). Internet is used increasingly for educational purposes. Additionally, computer network use has become a way of life for the majority of first-year students (Sax et al., 1998).

According to Green (1998), the Campus Computing Project's survey demonstrated that computer technologies have become major components of the campus environment and the college experience. Students regularly use Internet at schools, computer laboratories, libraries and community centres. Most of them access library catalogues, online databases, and other academic resources to complete a wide range of academic tasks (Green, 1998; Romiszowski & Mason, 1996; Browne et al., 2000; Shackleford et al., 1999).

Many institutions are requiring students to have computers to take advantage of Web-accessible classrooms by incorporating ICT courses into their curriculum (Gunaratne & Lee, 1996; Perry et al., 1998; Shelton et al., 1999; Sutherland & Stewart, 1999). The advantages of incorporating advanced technologies into instruction are more efficiently accomplishing new or existing tasks and, preparing students for the job market as well as enhancing productivity (Albright & Graf, 1992; Witmer, 1998; Maslin et al., 2008, 2009).

Along with information technology (IT) development, however, is the increasing numbers of unethical acts have been observed throughout the world (Mason, 1986). It has been realized that information security is not just a technology problem (Hassel & Wiedenbeck, 2004). The threats to information security can influence IT users' perception and behaviour (Huang et al., 2008). In fact, information security involves both technology and people, and it is becoming increasingly evident that "the human factor is the Achilles heel of information security" (Gonzalez & Sawicka, 2002).

1.3 STATEMENT OF THE PROBLEM

The development of information security remains a difficult process with uncertainty to protect personal and sensitive information from cyber-attacks. Numerous sophisticated security methods have been developed, but information security is declining (Turner et al., 2006). No matter how well designed, security methods rely on individuals to implement and use them. Technological solutions are important but not adequate (Rhodes, 2001). The success of security also depends on the effective behaviour of individuals (Cox et al., 2001; Stanton et al., 2003).

Internet provides students quick access to a large number of information sources. Students always use Internet not only for their academic purposes but also for personal purposes such as keeping in touch with their friends via e-mail, chatting, and blogs. Yet, along with these sources, the Web also contains millions of other Web sites that are operated by individuals, businesses, advocacy groups, clubs, and so on, which may offer inaccurate or biased information (Metzgera et al., 2003).

Students may not be aware to protect their computers from security attacks while they are browsing the Internet and thus lead to illegal access to their personal information or identity theft. With this proliferation of use, however, information and computer security are becoming important issues (Chai et al., 2006; Huang et al., 2008). Therefore, it is essential for a better understanding of IT users' attitude and behaviour on what they perceive, why they perceive it, and how they will subsequently behave in information security (Huang et al., 2008).

However, not much research has been done to explore the behavioural aspects of students on information security issues generally, while none has been done among International Islamic University Malaysia (IIUM) students in particular. Thus, the purpose of this research is to investigate the university student on information security behaviour and examine factors that influence university student's behaviour towards information security using IIUM students as case study.

1.4 RESEARCH QUESTIONS

This research focuses on factors that influence student's behaviour towards information security. The research questions were formulated for the purpose of this study and answers to these questions will hopefully provide the tentative factors on university student's information security behaviour.

There are a number of research questions have been made to guide the study. The study seeks to answer to the following research questions:

i. What are the factors that contribute to information security behaviour of university students?

   a. Is there a significant relationship between student’s attitude towards information security and information security behaviour?
   b. Is there a significant relationship between subjective norm and information security behaviour?
   c. Is there a significant relationship between student’s self-efficacy on information security and information security behaviour?
   d. Is there a significant relationship between perceived information security importance and information security behaviour?
   e. Is there a significant relationship between year of computer and Internet experience, and information security behaviour?
   f. Is there a significant relationship between duration of computer and Internet use, and information security behaviour?
   g. Is there a significant relationship between level of computer and Internet experience, and information security behaviour?
   h. Is there a significant relationship between level of information security experience, and information security behaviour?

1.5 RESEARCH OBJECTIVES

The purposes of this research are as follows:

i. To investigate the university student’s behaviour towards information security.

ii. To examine the factors contributing to information security behaviour.

1.6 RESEARCH MODEL

The research model in this study was adapted from previous study (Ng & Mohammad Azree, 2005; Chai et al., 2006) which focused on the factors that influence computer user’s to pay attention and practice computer security. The Figure 1.1 shows the theoretical model for this study which will later be modified to focus on factors that are likely to influence university students (as users) towards information security behaviour.

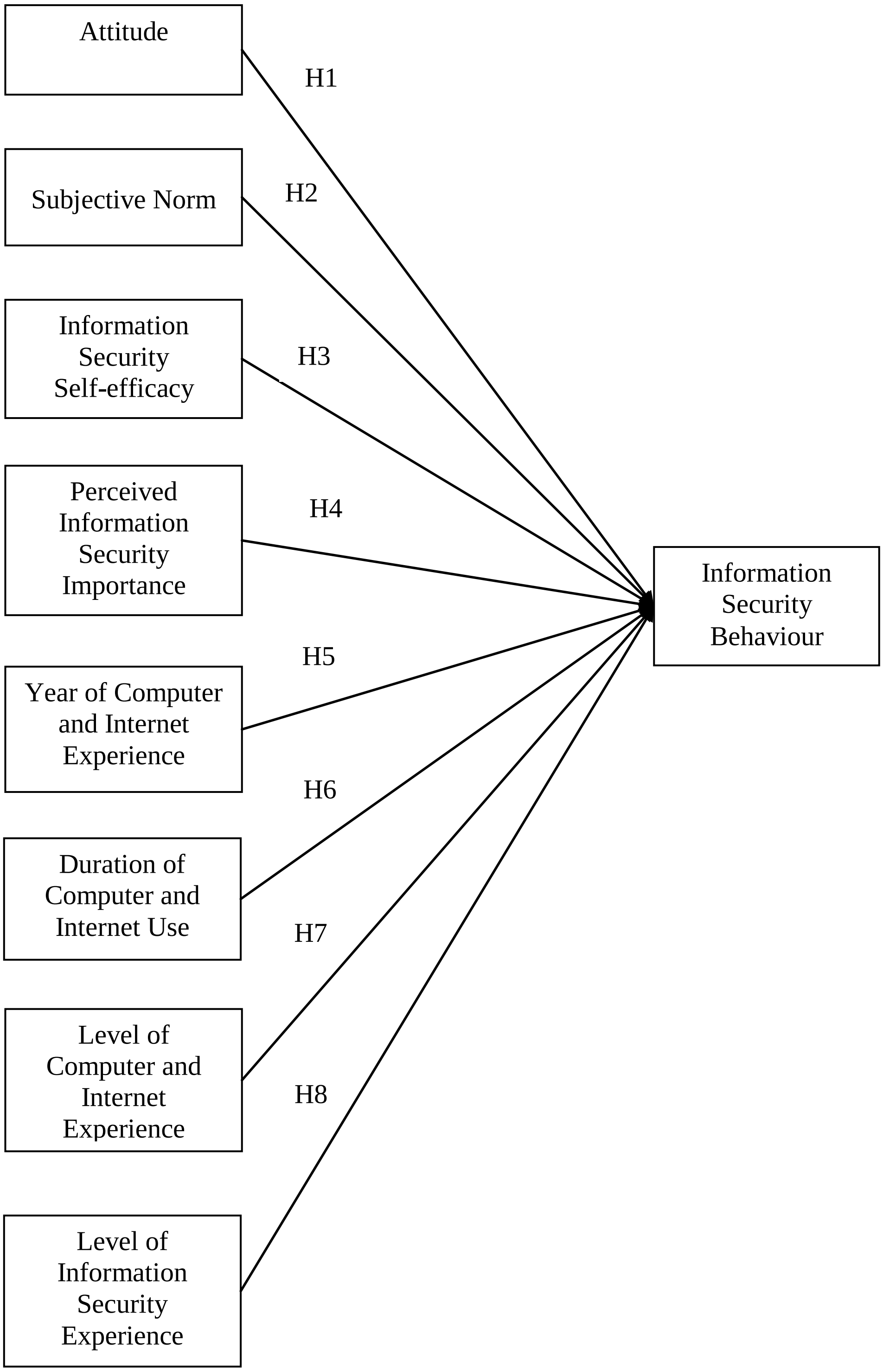
Attitude
Subjective Norm
Information Security Self-efficacy
Perceived Information Security Importance
Year of Computer and Internet Experience
Duration of Computer and Internet Use
Level of Computer and Internet Experience
Level of Information Security Experience
Information Security Behaviour
H1
H2
H3
H4
H5
H6
H7
H8

Figure 1.1: Research Model

1.7 RESEARCH HYPOTHESES

The hypotheses of this research are as follows:

H1: Attitude towards information security has positive relationship with information security behaviour.

H2: Subjective norm has positive relationship with information security behaviour.

H3: Information security self-efficacy has positive relationship with information security behaviour.

H4: Perceived information security importance has positive relationship with information security behaviour.

H5: Year of computer and Internet experience has significant relationship with information security behaviour.

H6: Duration of computer and Internet use has significant relationship with information security behaviour.

H7: Level of computer and Internet experience has significant relationship with information security behaviour.

H8: Level of information security experience has significant relationship with information security behaviour.

1.8 DEFINITION OF TERMS

The terms repeatedly used in this research are conceptually defined as follows:

1.8.1 Information Security

This refers to any process, activity, or task that protects the confidentiality, integrity, and accessibility of information (NIST, 1995; Parker, 1998; Tudor, 2002).

1.8.2 Information Security Behaviour

Behaviour can be defined as an individual's observable response in a given situation with respect to a given target (Ajzen, 1985). Information security behaviour is a user’s behaviour in protecting computer from virus attacks or security breaches.

1.8.3 Attitude

Attitude is an individual’s positive or negative evaluation of self-performance of the particular behaviour (Ajzen, 1985). In this study, it refers to a computer user responding positively or negatively towards information security.

1.8.4 Subjective Norm

Subjective norm is an individual's perception of the social pressure to perform or not to perform the behaviour under consideration (Ng & Mohammad Azree, 2005). With respect to security functionality, this relates to a person being influenced base on assumption of what others believe with respect to how he or she should behave towards information security.

1.8.5 Information Security Self-efficacy

Self-efficacy is an individual’s self-confidence in his ability to perform behaviour (Bandura, 1997). For this study, information security self-efficacy refers to an individuals’ judgment of their capabilities or skills performing information security behaviour.