UNDERSTANDING CONSUMER ADOPTION AND SECURITY OF INTERNET BANKING: A PROPOSED BIOMETRICS TECHNOLOGY IMPLEMENTATION IN THE MALAYSIAN BANKING CONTEXT

NORMALINI BINTI MD KASSIM

UNIVERSITI SAINS MALAYSIA

2013

UNDERSTANDING CONSUMER ADOPTION AND SECURITY OF INTERNET BANKING: A PROPOSED BIOMETRICS TECHNOLOGY IMPLEMENTATION IN THE MALAYSIAN BANKING CONTEXT

By

NORMALINI BINTI MD KASSIM

Thesis submitted in fulfillment of the requirements

for the degree of

Doctor of Philosophy

OCTOBER 2013

Dedication

With lots of love and respect to:

My mother Maznah Binti Mansoor,

My father Md Kassim Bin Pawanchik,

My husband Mohamad Naim Bin Osman and our children,

And my brothers.

I would like to dedicate this work

Acknowledgements

In the name of Allah, the Most Gracious, the Most Merciful. All praise to the Almighty, the One who has responded to my prayers in various ways and blessed me with patience, courage and fortitude throughout this research.

I would like to express my sincere and heartfelt appreciation to my supervisor Professor T. Ramayah for his constructive criticism and assistance throughout this work. This research has benefited from his guidance, advice, concern and encouragement.

I also would like to express my gratitude to the Dean of the Management School, Professor Fauziah Binti Md Taib and the Deputy Dean, Professor T. Ramayah along with other Management School staff for their help throughout the course of this work.

My sincere thanks also to all members of the Management School for their cooperation, constructive discussion and friendly environment that helped me in many ways in completing this study. I am also grateful to Universiti Sains Malaysia for providing me a place to pursue my higher studies.

Many people have challenged and influenced my thinking throughout this research, especially my friends Wan Normila, Fardzah Sulaiman, Zunirah Mohd Talib, Dr Thien, Roshni Ann George, Santhanamery and Ainul Mohsein. Special thanks to all the respondents and others who directly or indirectly helped me in this study.

Last but not least, my very special admiration to my parents, my husband and my children for their love, patience, and encouragement.

TABLE OF CONTENTS

CHAPTER 2 : LITERATURE REVIEW

LIST OF TABLES **Page**

LIST OF FIGURES **Page**

LIST OF FIGURES (Continued) **Page**

LIST OF ABBREVIATIONS

AMOS	Analysis of Moment Structures
APWG	Anti Phishing Working Group
AVE	Average Variance Extracted
BAFIA	Banking and Financial Institution Act
CBSEM	Covariance-based structural equation modeling
CFA	Confirmatory Factor Analysis
CMV	Common Method Variance
CR	Composite Reliability
DOPU	Drop-off and pick-up
EFA	Exploratory Factor Analysis
EM	Expectation Maximization
GOF	Goodness of Fit
MYCERT	Malaysian Computer Emergency Response Team
PLS	Partial Least Squares
SEM	Structural Equation Modeling
SPSS	Statistical Package for the Social Sciences
SSL	Secure Sockets Layer
TAC	Transaction Authorization Code
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action
UTAUT	Unified Theory of Acceptance and Use of Technology

LIST OF APPENDICES

Page

LIST OF PUBLICATIONS

1. Normalini Md Kassim and T. Ramayah (2010). Security Policy Issues in Internet Banking in Malaysia. Handbook of Research on Information Communication Technology : Trends, Issues and Advancements, Editor: Esharenana E. Adomi, IDEA Group International (IGI Global), Chapter 42, 667-687. ISBN13:9781615208470. IDEA Group International.

2. Normalini, M.K. and T. Ramayah (2012). Biometrics Technologies Implementation in Internet Banking Reduce Security Issues? Procedia – Social and Behavioral Sciences, 65, 364-369. (ELSEVIER) (SCOPUS)

3. Normalini Md. Kassim, T. Ramayah and Sherah Kurnia (2012). Antecedents and Outcomes of Human Resource Information System (HRIS) Use. International Journal of Productivity and Performance Management, 61 (6), 603-623. (EMERALD) (SCOPUS)

4. Normalini Md. Kassim and T. Ramayah (2013). Understanding Security iin Consumer Adoption of Internet Banking: Biometrics Technology Implementation in the Malaysian Banking Context. Handbook of Research and Development in E-Business through Service-Oriented Solutions, Editor: Katalin Tarnay, Sandor Imre & Lai Xu, IDEA Group International (IGI Global), Chapter 15, 293-306.ISBN: 9781466641815.

In Print

1. Normalini, M.K. and T. Ramayah. Perceived Risk Factors Influence on Intention to Continue Using Internet Banking Among Malaysians – Journal of Consumer Behaviour

MEMAHAMI PENERAPAN PENGGUNA DAN KESELAMATAN PERBANKAN INTERNET: SATU CADANGAN PELAKSANAAN TEKNOLOGI BIOMETRIK DALAM KONTEKS PERBANKAN MALAYSIA

ABSTRAK

Kajian ini mengkaji lanjutan Model Penerimaan Teknologi (TAM) sebagai model berasaskan penerimaan sistem maklumat dalam konteks perbankan Internet. Dalam usaha untuk menyediakan teori asas yang kukuh tentang keinginan menggunakan aplikasi perbankan Internet, kajian ini mencadangkan TAM dilanjutkan dengan dimensi kualiti sebagai pembolehubah luaran dalam TAM dan tanggapan risiko sebagai pembolehubah kepercayaan tambahan dan model perbankan e-kepercayaan (e-trust). Model ini mengabungkan tiga dimensi utama untuk mengenalpasti faktor yang mempengaruhi keinginan untuk terus menggunakan perbankan Internet; kualiti, risiko tanggapan dan tanggapan keselamatan dengan keberkesanan tanggapan penggunaan teknologi biometrik dan persepsi kebolehpercayaan sebagai moderator. Sejumlah 413 pengguna perbankan Internet di Pulau Pinang, Selangor, Kuala Lumpur dan Johor yang mewakili penduduk di Semenanjung Malaysia telah menyertai tinjauan kaji selidik ini**.** Temuan kajian menunjukkan kualiti sistem, kualiti maklumat dan kualiti perkhidmatan mempunyai kesan positif yang signifikan terhadap persepsi kebergunaan. Manakala risiko fizikal dan risiko sosial mempunyai kesan negatif yang signifikan ke atas sikap terhadap penggunaan perbankan Internet. Walau bagaimanapun, risiko fungsian, risiko kehilangan masa, risiko kewangan, risiko peluang kos dan risiko maklumat tidak mempunyai pengaruh negatif yang signifikan ke atas sikap penggunaan perbankan Internet. Hasil kajian ini juga menunjukkan persepsi kemudahan penggunaan tidak

mempunyai kesan signifikan ke atas sikap terhadap penggunaan perbankan Internet manakala persepsi kegunaan mempunyai kesan positif yang signifikan ke atas sikap terhadap penggunaan perbankan Internet. Selain itu, persepsi privasi telah terbukti tidak mempunyai kesan signifikan ke atas kepercayaan pengguna perbankan Internet. Hasil kajian juga mendapati bahawa pengesahan, kerahsiaan, integriti data dan "non-repudiation" mempunyai kesan positif yang signifikan ke atas kepercayaan pengguna perbankan Internet. Selain dari itu, didapati bahawa persepsi integriti dan persepsi kemuliaan dianggap tidak mempengaruhi hubungan di antara persepsi privasi dan kepercayaan pengguna perbankan Internet. Penemuan kajian juga menunjukkan persepsi kecekapan mempengaruhi hubungan di antara "non-repudiation" dan kepercayaan pengguna perbankan Internet. Walau bagaimanapun, persepsi kecekapan tidak mempengaruhi hubungan di antara pengesahan, kerahsiaan dan integriti data terhadap kepercayaan pengguna perbankan Internet. Penemuan kajian jelas menunjukkan bahawa persepsi keberkesanan penggunaan teknologi biometrik mempengaruhi hubungan di antara kerahsiaan dan integriti data terhadap kepercayaan pengguna perbankan Internet. Walau bagaimanapun, persepsi keberkesanan penggunaan teknologi biometrik tidak mempengaruhi hubungan di antara pengesahan dan "non-repudiation" terhadap kepercayaan pengguna perbankan Internet. Di samping itu, penemuan kajian berjaya mengesahkan bahawa kepercayaan mempunyai kesan positif yang signifikan terhadap keinginan untuk terus menggunakan perbankan Internet dan sikap terhadap menggunakan perbankan Internet. Seperti jangkaan, sikap terhadap penggunaan perbankan Internet mempunyai kesan positif yang signifikan terhadap keinginan untuk terus menggunakan perbankan Internet.

UNDERSTANDING CONSUMER ADOPTION AND SECURITY OF INTERNET BANKING: A PROPOSED BIOMETRICS TECHNOLOGY IMPLEMENTATION IN THE MALAYSIAN BANKING CONTEXT

ABSTRACT

This study extends the Technology Acceptance Model (TAM) to a model that is based on information system acceptance in an Internet banking context. To provide a solid theoretical basis, the study proposed that the TAM be extended with quality dimensions (as external variables), perceived risk (as an additional belief variable) and the model of e-trust banking. The model incorporates three main dimensions to identify factors influencing intention to continue using Internet banking; Quality, Perceived Risk and Perceived Security which is moderated by Perceived Effectiveness of Biometrics Technology Usage and Perceived Trustworthiness. A total of 413 respondents (Internet banking customers) from Penang, Selangor, Kuala Lumpur and Johor (participated in this study). The findings show a significant positive effect of System Quality, Information Quality and Service Quality on Perceived Usefulness while Physical Risk and Social Risk had a significant negative influence on attitudes towards the use of Internet banking. However, Functional Risk, Time Loss Risk, Financial Risk, Opportunity Cost Risk, and Information Risk had no significant negative influence on attitudes towards the use of Internet banking. The results also illustrate that Perceived Ease of Use had no significant impact on the attitude towards the use of Internet banking while Perceived Usefulness had a significant positive impact. Besides that, Perceived Privacy was proven to have no significant impact while Authentication, Confidentiality, Data Integrity, and Non-repudiation have a significant positive impact on customers' trust in Internet banking. Furthermore, Perceived Integrity and Perceived Benevolence do

not moderate the relationship between Perceived Privacy and customers' trust in Internet banking. Findings also show that Perceived Competence moderates the relationship between Non-repudiation and customers' trust in Internet banking. However, Perceived Competence does not moderate the relationship between Authentication, Confidentiality and Data Integrity towards customers' trust in Internet banking. Perceived Effectiveness of Biometrics Technology Usage was clearly shown to moderate the relationship between Confidentiality and Data Integrity towards customers' trust in Internet banking. However, Perceived Effectiveness of Biometrics Technology Usage did not moderate the relationship between Authentication and Non-repudiation towards customers' trust in Internet banking. In addition, it has been confirmed that trust has a significant positive impact on intention to continue using Internet banking and attitude towards the use of Internet banking. As expected, attitude towards the use of Internet banking has a positive influence on intention to continue using Internet banking.

CHAPTER 1

INTRODUCTION

1.0 Introduction

A huge new market for Internet-based services such as Internet banking was offered and the global Internet users exceeded 2267 million people in December 2011 (IWS, 2012). Traditional banking practice has transformed to Internet banking growth in many countries, since new millennium. Lower the operational costs, consumer banking services improved, consumers retained and expand their share of customers can be offered by Internet banking services (Sharman Lichtenstein & Williamson, 2006). Expense ratio of 15% to 20%, which is operational rate for Internet based banks compared to 50% to 60% for the average bank (Booz, Allen, & Hamilton, 1997). Operating costs would be saved by encouraging customers to use the Internet banking services. Banks require offering Internet banking due to competitive pressures. Online banking market would be interested to enter by new players such as software and telephone companies (Hagel & Eisenmann, 1994; Hagel & Lansing, 1994). Therefore, the expectation for Malaysian banks would not be fast providing Internet banking services but would encourage customers to transform to this form of delivery of bank services.

As for multi-channel strategy, Internet banking was managed as an operational activity in the new banking environment (Black, Lockett, Ennew, Winklhofer, & McKechnie, 2002). Internet is an open environment and it has brought the information superhighway to our doorstep. Therefore, online applications are exposed to security threats such as scams, phishing, and password-sniffing.

Sathye (1999) highlighted that the security concern and benefit of the system awareness are the main obstacle in Australia. The major source of apprehension about Internet banking were security concerns, which the facts by the survey conducted in the USA concluded that 67% of the banks surveyed agreed (Thorton, 1996).

Security threats owing to network and data transactions and account access with authentication failure were security concerns in Internet banking. Customers‟ perception of the level of protection against security threats can be recognized as "perceived security" (Yousafzai, Pallister, & Foxall, 2003). Figure 1.1 shows the structure at the core of e-commerce security for Internet banking. The diagram shows how an acceptable level of trust is established for parties in a transaction by the use of appropriate authentication mechanisms.

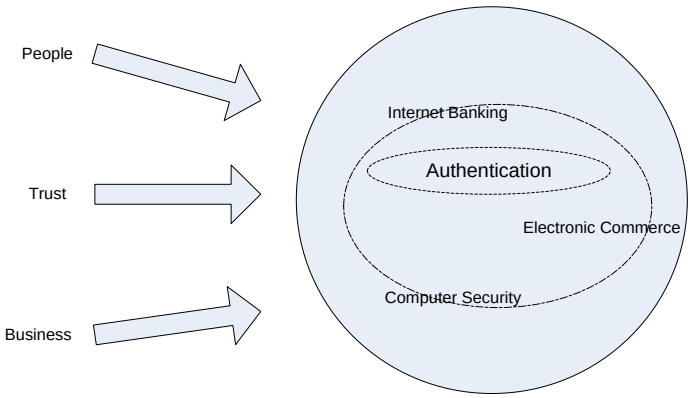


Figure 1.1 Internet banking security issues. Source adapted from Hutchinson and Warren (2003).

Customers are apprehensive about the security of their personal financial information that could be accessed via the Internet. The electronic banking community recognized the security needs. A number of technologies have been developed to ensure the security of electronic transactions. The 128-bit RSA

encryption key technology to web browsers is the most common approaches used to secure online transactions in the use of digital certificates and firewalls.

The key factors influencing customer adoption in Internet banking can be define in this study. Many studies conducted in Malaysia and other countries, which identified the trend of Internet banking growth adoption in Malaysia. Adoption of Internet banking in Malaysia and slow growth due to security and personal preferences factors (Suganthi, Balachandher, & Balachandran, 2001). In Australia, the main obstacles to Internet banking adoption are due to security concerns and Internet banking awareness (Sathye, 1999). Furthermore, the safety and security of transactions over the internet were concerned by Internet banking customers in Australia.

Ramayah, Ismail and Koay (2002) identified the following six external variables that influence Internet banking adoption among Malaysian consumers namely, prior experience, training, perceived risk, awareness, cost and external pressure. This study highlighted the fact that the majority of respondents not using Internet banking. Another study by Rouibah, Ramayah, and Oh (2009) found that the direct positive effect relationship between five factors (perceived ease of use, perceived usefulness, attitude, subjective norms and perceived behavioural control) and behavioural intention to use. This study revealed that the model has the best explanatory power was the Theory of Planned Behaviour (TPB), followed by Theory of Reasoned Action (TRA) and Technology Acceptance Model (TAM) models. A unique study in Malaysia with regards in Internet banking areas which compares three models has been presented in this research. However, TAM model has the best

explanatory power, followed by TPB and TRA models (Rouibah, Ramayah, & Oh, 2011).

Raju, Thiagarajan, and Seetharaman (2007) studied the extent of decision to adopt and the growth of the Internet banking services by Malaysian consumers. A study conducted by Marhana, Fadzli, and Zakaria (2012) revealed that a majority of Muslim consumers have not used Internet banking due to the fact that some people still have no opportunity to use the service and they are unsure of the security of such a service. Hanudin and Ramayah (2010) found that Perceived security and privacy (PSP) was one of the key factors to determine a bank customer‟s intention to use SMS banking.

Thomas, Kellermann, and McNevin (2002) highlighted the fact that value is added by the electronic security to an open network. Infrastructure, both soft (policies, processes, protocols, and guidelines that protect the system and data) and hard (hardware and software needed to protect the system and data) constitutes the structure of electronic security. Thomas et al. (2002) stated that technology creates the opportunity for violations and infringements to take place quickly even though such technology results in the expanding of scope and timing proportions for transactions. Before the rise of technology in Internet banking, highly organized criminals would need months or sometimes years to pilfer fifty thousand credit card numbers. In recent times, a single person is able to illegally enter databases and pilfer the same amount of credit card information in seconds using Web related devices. Hence, e-security should be considered seriously in this day and age due to possibilities such as these (Thomas et al., 2002).

Computers are highly depended on in the banking and financial industries; even so, it was these industries that reported the highest incidence of misuse amounting to 57% (Hutchinson, 2000). Citibank recorded a security breach in the 1990s which was considered by banking and security circles as one of the successful electronic bank frauds (Barlotta, 1999). The fraud resulted in Citibank‟s security system being penetrated by hackers who wired USD10 million to banks around the world in September 1994, whereby USD 400,000 was recovered. One of the newer security threats for computers, "NMAP", can be hacked by just a single hacker instead of hundreds operating around world (Barlotta, 1999).

Since further information to better understand Internet banking in Malaysia is needed, this research investigates the effect of the security and trust on customer‟s intention to continue Internet banking**.** The relationship between each of the security requirement factors such as authentication, non-repudiation, confidentiality, and data integrity with customers‟ trust in using Internet banking is also examined in this research. Beside, whether or not perceived trustworthiness and perceived effectiveness of biometrics technologies usage moderates the relationship between security and trust towards intention to continue using the Internet banking system will be investigated as well.

1.1 Background of the Study

The Malaysian banking sector is under the supervision of Bank Negara Malaysia and is licensed under the Banking and Financial Institutions Act 1989 (BAFIA). The sector includes commercial and merchant banks, finance companies, discount houses and money brokers which act as financial intermediaries (BNM,

2009b). The banking sector accounted for about 70% of the total assets in the financial system at the end of 1999 and is the primary source of financing for the domestic economy. The sector comprised of twenty seven commercial banks (19: 100% owned by foreign entities and 8:100% owned by local entities) in the year 2012 (BNM, 2012). Thereafter, there was a merger of domestic banking institutions which significantly reduced the number to ten commercial banks, ten finance companies and nine merchant banks. Currently, about 75% of the banking sector"s market share (total assets and total deposits) are controlled by domestic banking institutions (excluding the discount houses) (BNM, 2009b).

The banking sector is being transformed by developments in telecommunications and information technology. Electronic banking has become the ultimate service delivery system to fulfill the needs of banking customers due to the explosive expansion of the Internet and computer usage. The Malaysian government has structured a legal framework for Internet banking services as a result of the competitive nature of the banking sector.

The Malaysian Central Bank authorized domestic commercial banks on 1st of June 2000, to offer Internet banking services. The largest domestic bank in Malaysia, Maybank, became the first Malaysian bank to offer Internet banking services on June 15th 2000. By the seventh of August 2002, eight Malaysian commercial banks started providing Internet banking services, including (Suganthi et al., 2001):

- Alliance Bank Malaysia Berhad
- Ambank Berhad

- Bumiputra-Commerce Bank Berhad
- Hong Leong Bank Berhad
- Malayan Banking Berhad
- Public Bank Berhad
- RHB Bank Berhad
- Southern Bank Berhad

At the moment, banks that are permitted to provide Internet banking services in Malaysia have to be licensed under the Banking and Financial Institution Act 1989 (BAFIA) and the Islamic Banking Act 1983. Presently, Bank Negara Malaysia has registered twenty two commercial banks consisting of nine Malaysian banks and thirteen foreign banks. The nine Malaysian owned banks that are registered to offer Internet banking services are listed in Table 1.1.

Table 1.1

Internet Banking Services Provider

No.	Banks	Service Websites	Services Transactions
1	Affin Bank Berhad	www.affinbank.com.my	• Check account balance and statement. • Submit applications for new accounts, credit cards or loan • Place fixed deposits • Transfer funds between accounts (own and third party) intra bank or interbank GIRO • Bill payments, credit cards, loans and insurance premium • Create, change and cancel standing orders • Request for cheque books and statements • Check status or stop payment of your cheques • Apply for bank drafts and telegraphic transfer
2	Alliance Bank Malaysia Berhad	www.alliancebank.com.my	
3	Ambank (M) Berhad	www.ambg.com.my	

Notes. Source taken from BNM (2009a)

Table 1.1 (Continued)

No.	Banks	Service Websites	Services Transactions
4	CIMB Bank Berhad	www.cimbclicks.com.my	• Account Enquiry (check balance and statement) • Transfer funds (interbank GIRO or intra bank) own and third party • Pay bills • Prepaid reload and online Games reload • Western Union • Remittance • Account opening • Standing instructions • Mobile banking • Unit trust, Share trading and eIPO • Cheque management • Air Asia Bidding • EPF • eApplication • Risk Profiler
5	EON Bank Berhad	www.eonbank.com.my	• Check account balance and statement. • Submit applications for new accounts, credit cards or loan • Place fixed deposits • Transfer funds between accounts (own and third party) intra bank or interbank GIRO • Bill payments, credit cards, loans and insurance premium • Create, change and cancel standing orders • Request for cheque books and statements • Check status or stop payment of your cheques Apply for bank drafts and telegraphic transfer
6	Hong Leong Bank Berhad	www.hlb.com.my	
7	Malayan Banking Berhad	www.maybank2u.com.my	• Accounts & Banking view and manage your accounts, make payments and transfer funds • Investment – trade using online stocks, purchase additional Amanah Saham Nasional Berhad Unit trust and manage other investments. • Insurance – renew your insurance policy or purchase insurance online • Loans – view and manage your home or car loans • Mobile banking – signup for and manage your mobile banking accounts • Personal details – change password or manage your personal details. • Buy online – Reload your mobile, Internet or IDD/STD prepaid, or buy a starter pack • Maybank @ SG – access your Maybank Singapore account • Bills & Statements – View your bills, bank statements & advises.

Table 1.1 (Continued)

No.	Banks	Service Websites	Services Transactions
8	Public Bank Berhad	www.pbebank.com	• Check account balance and statement. • Submit applications for new accounts, credit cards or loan • Place fixed deposits • Transfer funds between accounts (own and third party) intra bank or interbank GIRO • Bill payments, credit cards, loans and insurance premium • Create, change and cancel standing orders • Request for cheque books and statements • Check status or stop payment of your cheques Apply for bank drafts and telegraphic transfer
9	RHB Bank Berhad	www.rhb.com.my	

Notes. Source taken from BNM (2009a)

Internet banking subscription in 2002 for the two leading banks offering such services in Malaysia, Maybank and HSBC, amounted to 25,000 and 10,000 customers respectively (Yu, 2002). In Malaysia, adoption of Internet banking is comparatively low and the main determinants for adoption have not been researched much. In Malaysia, adoption of Internet banking is comparatively low and the main determinants for adoption have not been researched much. This can be supported by Zanariah, Hawati Janor, Rajendraan, Noorli Khamis and Shamsuri (2013) and Murali Raman, Richard Stephenaus, Nafis Alam, and Kuppusamy (2008) who categorized Malaysia as among the developing countries and the recent statistics show that the adoption of Internet banking in Malaysia is still low in spite of various initiatives made by financial institutions to attract users. Despite all the advantages of Internet banking, studies by Hari Mohan et al. (2013) and Noorizan, Raja Munirah, and Norfazlina (2012), suggests that general usage of Internet banking is still not in line with the growth of the Internet banking services in Malaysia. Hence, Internet banking development is still at the early phase though the electronic transformation

has begun in Malaysia. Furthermore, the banking industry is finding it difficult to improve the dissemination of Internet banking (Ndubisi & Sinti, 2006).

Comprehensive research in the area of e-banking issues and customer preferences has not taken off from a Malaysia perspective even though many studies have been carried out to investigate issues of e-banking and customer loyalty in other countries. However, there has been a study conducted to examine e-banking development in Malaysia whereby various electronic delivery channels were also examined such as automated teller machines (ATM), telebanking and PC banking (Balachandher, Santha, Norhazlin, & Rajendra, 2000). The factors that have an effect on e-banking adoption in Malaysia were also analyzed in another study (Suganthi et al., 2001).

According to Sohail and Shanmugham (2003), Internet ease of access, e-banking awareness, and customers‟ unwillingness to change are the factors that considerably influenced the practice of e-banking in Malaysia. The study on e-banking adoption and customer preferences determined that several crucial psychological and behavioural issues in trust, security, customers‟ unwillingness to change and a preference for human interactions had to be addressed even though e-banking offered new prospects in the banking industry.

There are a few security issues occurring in Malaysian Internet banking such as Online Identity Fraud or Phishing. *Phishing* or online pilfering of identity is the malevolent attempt of baiting mass audiences into misleading websites by thousands of emails sent by fraudsters. Criminals create websites that appear to be from trusted organizations and blast deceptive emails to random email addresses in an attempt to commit online identity fraud or *Phishing*. Connections to websites that appear to be

similar to the websites of real organizations deceive customers into providing precision information such as user IDs, passwords, and TACs. Criminals are able to access the customer‟s bank account by using this personal information. Few examples for different types of phishing as published in the CIMB website at www.cimbclicks.com.my/keepsave.htm are given next:

a) Phishing Emails/Mules

People who take delivery of stolen money from phishing victims are known as money mules. When criminals want to hide their tracks, money mules offer a good solution. Before funds are sent out of the country, mules act as the transit or intermediate agents. Hence, the hidden side of phishing is that money mules are used to cover tracks. Offline components of online phishing consist of illegal money laundering syndicates. Worldwide money laundering has resulted in increasing phishing and identity theft.

b) Phishing SMS

Irresponsible people will send to the victim an SMS to get the account details and confidential data from the victim. The following is the phishing SMS example taken from CIMB clicks website. (Source taken from CIMB Bank (2012)):

> Congratulations! This SIM card has won RM7,000 from AFM (Academy Fantasia Malaysia 4) and will be sent a cheque. An account with BCB is required to be opened and deposited with RM1,000 using an ATM card. This number can be contacted for further details: 004 261 731 146 23.

c) Phishing Website

This phishing Website is the fake version of the actual website. They would look identical. The message on the website requires users to enter User ID, password and TAC.

d) Suspicious investment programmes

Please be cautious of appealing investment-like programmes or schemes, which are widely available via the internet. The bank does not endorse such programmes and is not in any way associated with them.

e) Online Currency

Online currencies or otherwise known as electronic currencies are widely used all over the world as an alternative online payment. There are several types of online currencies available in the market, with the most popular ones being:

- e-Bullion
- e-Silver
- e-Platinum
- e-Palladium
- e-Gold

1.2 Trends of Security Breaches

MyCERT or the Malaysian Computer Emergency Response Team operates a public service in the form of the Cyber999 Help Centre which provides emergency response to computer security issues in addition to support in management of

incidents such as computer abuses, hack attempts and other security breaches related to confidential information. The team is formed by experts including:

- Intrusion Analysts
- Malware Analysts
- Application Security Analysts
- Emergency Response Professionals

The summary report of MyCert Security Breaches (2005 - 2010) relating to computer security incident handling and trends observed from the research network provides an overview of activities carried out by MyCERT (2010). Incidents categories supported by MyCERT (from 2005 to 2010) are shown in Table 1.2. In general, cyber security incidents include, but are not limited to:

(a) Unauthorized access attempted to a computer system or its data

(b) Unwanted disruption or denial of service

(c) Unauthorized use of a system for processing or storing data

(d) Changes to system hardware, firmware, or software without the knowledge or consent of the system owner.

By and large, all categories show increasing trends in the number of reports every year. The majority of incidents recorded were due to fraud and intrusion representing 37% and 36% respectively for the year 2010, followed by malicious code at 20%, harassment at 7% and denial of service at 1%. Incidents related to system intrusion were generally caused by web defacement. The major reason for defacements was discovered by MyCERT to be related to vulnerable web

applications. Phishing sites of local and foreign institutions comprised most of the fraud related incidents (MyCERT, 2010).

Table 1.2

MyCERT Security Breaches (2005-2010)

	2005	**2006**	**2007**	**2008**	**2009**	**2010**
Harassment	43	63	68	72	174	419
Fraud	149	287	364	907	1022	2212
Malicious Code	82	68	182	277	283	1199
Denial of Service	7	6	8	12	28	66
Intrusion	467	897	385	766	1766	2160
TOTAL	748	1321	1007	2034	3273	6056

Notes. Data taken from MyCERT (2010)

Figure 1.2 and Figure 1.3 shows the security breaches trends for all categories from 2005 to 2010. The categories showed sharply increasing pattern from 2005 to 2010. Fraud is the highest incident with 2212 reports for year 2010. This was followed by intrusion with 2160 cases, malicious code with 1199 cases, harassment with 419, and denial of service with 66 reports for 2010.

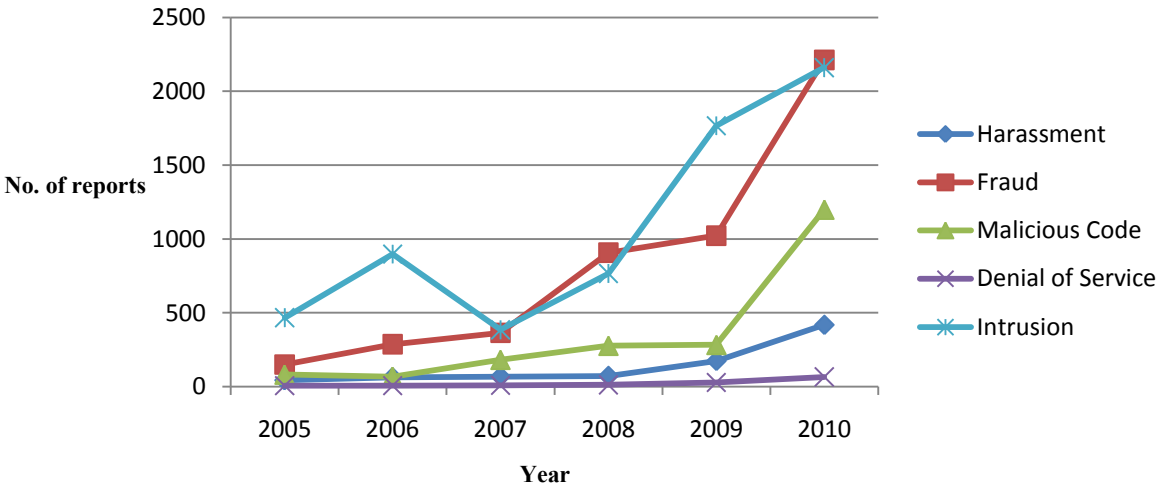


Figure 1.2 Security breach trends for all categories

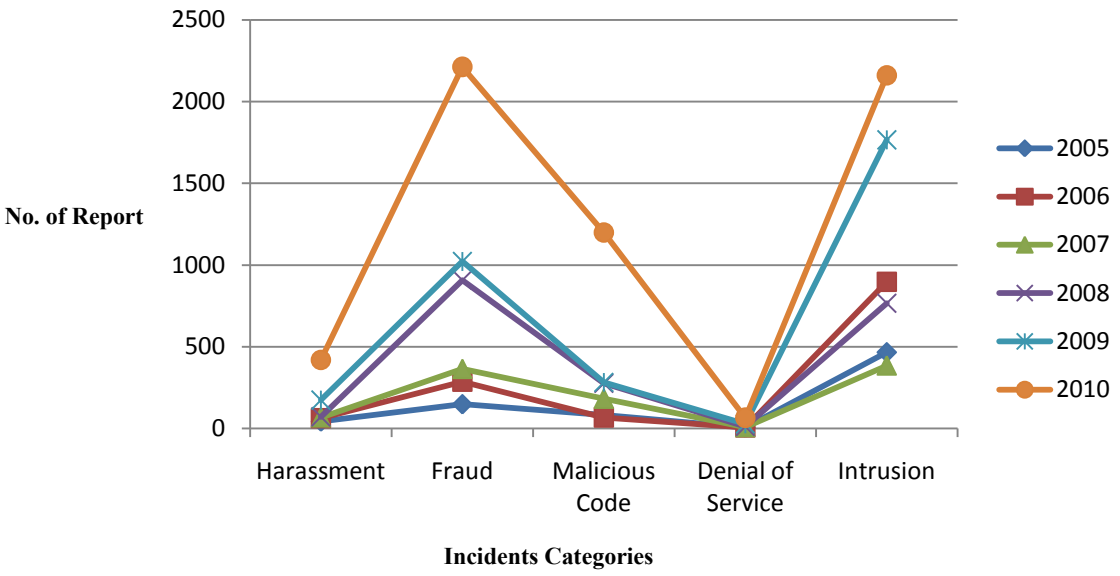
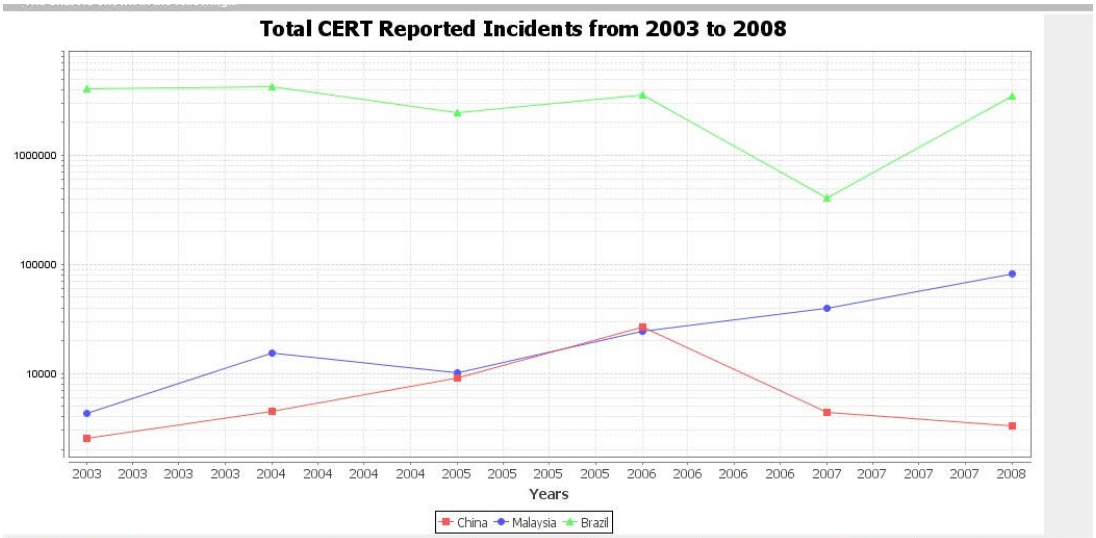


Figure 1.3 Security breach trends through the years (2005-2010)

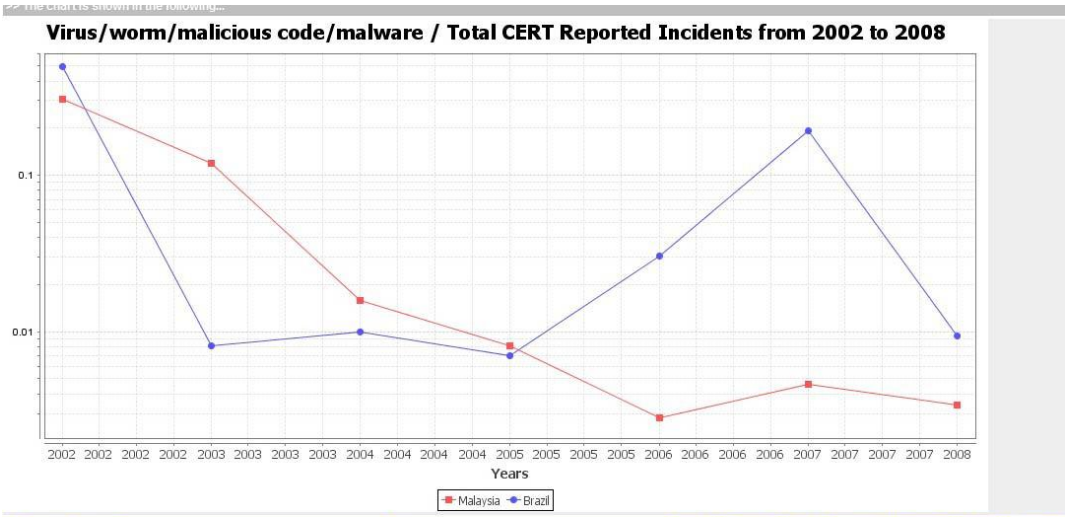
The total CERT occurrences from 2003 to 2008 reported in three countries, namely China, Malaysia, and Brazil are shown as a screenshot in Figure 1.4 (Madnick, Li, and Choucri, 2009). For most of the years, Brazil had a higher number of CERT incidents reported compared to China and Malaysia. The data component of China and Malaysia would shift to the bottom of the chart if a linear Y-axis scale is used due to the vast disparity.



Country/Region	Data	2003	2004	2005	2006	2007	2008
China	Total CERT Reported Incidents	2557.0	4485.0	9112.0	26476.0	4390.0	3291.0
Malaysia	Total CERT Reported Incidents	4295.0	15286.0	10147.0	24252.0	39639.0	82649.0
Brazil	Total CERT Reported Incidents	4126941.0	4232104.0	2482200.0	3601322.0	404695.0	3520501.0

Figure 1.4 Total CERT Reported Incidents from 2003 to 2008 (Logarithmic).

The Total CERT reported incidents of Malaysia and Brazil from 2002 to 2008 of "Virus/worm/malicious code/malware" is shown in Figure 1.5 as a screenshot of a chart with a logarithmic Y-axis scale. The data components in percentages of the "Virus/worm/malicious code/malware" category, which is one of the categories of the total reported CERT incidents, can be seen in this particular figure.



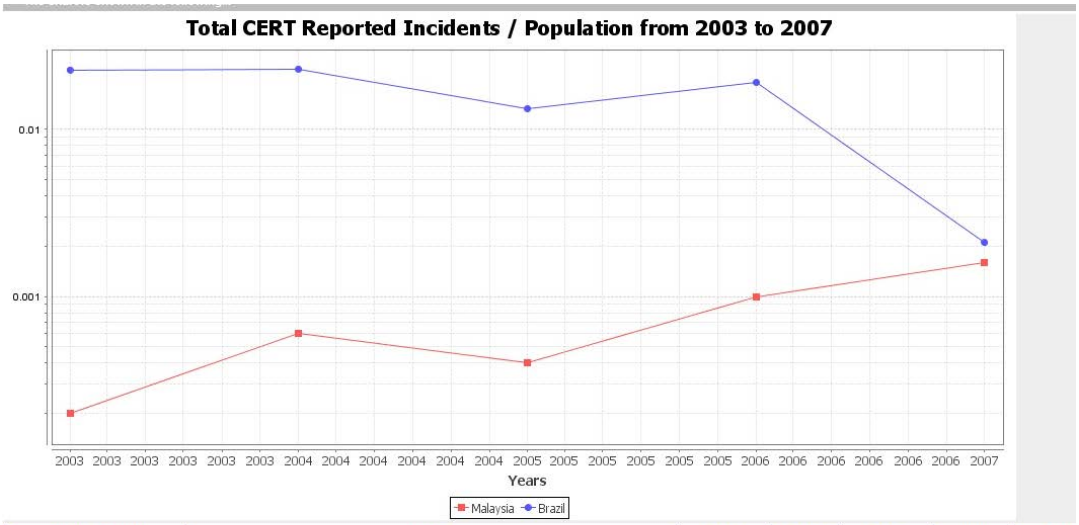
Country/Region	Data	2002	2003	2004	2005	2006	2007	2008
Malaysia	Virus/worm/malicious code/malware / Total CERT Reported Incidents	0.3045	0.1197	0.0158	0.0081	0.0028	0.0046	0.0034
Brazil	Virus/worm/malicious code/malware / Total CERT Reported Incidents	0.494	0.0081	0.01	0.0070	0.0305	0.1914	0.0094

Figure 1.5 Percentage of Virus/worm/malicious code/malware from 2002 to 2008 (Logarithmic)

A country comparison of Malaysia and Brazil can be found in Figure 1.6. The screenshot depicts the "Total CERT Reported Incidents" divided by the "Population" of those countries, from 2003 to 2007, using a chart with a logarithmic Y-axis. Hence, a per capita number of reported incidents is created whereby both countries start at very different levels in 2003, separated by about two orders of magnitude. However, by 2007, Brazil levels have dropped while Malaysia levels have risen whereby both rates have become almost equal. Madnick et al. (2009) questioned the reason for these statistics. There are two different hypotheses that can be put forward:

(a) Government and companies worked hard to reduce incidents in Brazil as there were high levels of incidences in 2003and consequently they have made progress to make a significant reduction.

(b) In 2003, Malaysia had relatively low levels of incidents as such similar efforts were not made, thereby resulting in increasing rates of incidents.



Country/Region	Data	2003	2004	2005	2006	2007
Malaysia	Total CERT Reported Incidents / Population	2.0E-4	6.0E-4	4.0E-4	0.0010	0.0016
Brazil	Total CERT Reported Incidents / Population	0.0227	0.023	0.0133	0.0191	0.0021

Figure 1.6 Total CERT Reported Incidents per Capita from 2003 to 2007 (Logarithmic)

There is a variation of data availability by category as precise definitions of cyber security data categories that are currently used by the CERTs are difficult to find. Furthermore, many countries do not have national CERTs even though these institutions are often the main sources of such cyber security data. In addition, CERTs are relatively new in several countries and most do not provide much data. Exploring cyber international relations will be a challenge if inadequate data availability continues.

1.3 Problem Statement

According to the Financial Fraud Action, UK (2010), in 2009 online banking fraud losses totaled £59.7 million which was the highest since 2004. This increase is due to a number of factors such as fraud activities. As well as an increase in phishing incidents, online banking customers are increasingly being targeted by malware attacks. Number of phishing websites targeted against UK banks and building societies were 51,161 in 2009, up from 43,991 websites in 2008. Other

types of scams called „money mule" which most of the fraudsters behind online banking are located overseas. There were an increment to 1,623 incidents of money mule in year 2008, compared with 1,462 in 2007.

Banks are seeking greater market expansion even as there has been significant Internet banking diffusion in many countries to date. At present, there is uncertainty in market growth trends due to rising identity fraud and online scams which are resulting in increased security concerns. The way banks deal with erroneous transactions and security concerns that may possibly occur during online banking will influence customer confidence in e-banking (Sohail & Shanmugham, 2003).

In 2002, there were approximately 800,000 Internet banking users in Malaysia with many new users signing up with their respective banks (Phang & Fernandez, 2002). Out of all the banks operating in Malaysia, Maybank had 600,000 registered users and the largest number of Internet banking customers (Phang & Fernandez, 2002). According to the 2008 survey on household use of the Internet by Malaysian Communications and Multimedia Commission, Internet banking usage in Malaysia was only at 31.8% in 2008.

According to recent studies by Raju, et al. (2007); Lu, Hsu, and Hsu (2005), Malaysian consumers strongly agree that the lack of security and reliability of transactions over the Internet are factors which cause Internet banking adoption to progress slowly. This is in line with the findings of management consultants McKinsey & Co in 2000, which discovered that only thirty one percent of Malaysians surveyed were interested in adopting Internet banking, whilst an

overwhelming 66% cited security and risk as their major concerns (Ng, 2002). Hence, banks have to make important improvements to address consumer concerns and increase Internet banking demand.

Suganthi et al. (2001) conducted a study which found that security concerns were one of the important factors influencing Internet banking in Malaysia. This finding was also supported by another study in the country whereby most individuals were found to be reluctant to apply Internet banking due to security and privacy issues (Ramayah et al., 2002). The main issues regarding Internet banking in Malaysia are the weak security and trustworthiness in adopting internet banking applications. Therefore, this study seeks to investigate risk and security requirement factors that impact Internet banking application adoption.

1.4 Research Objectives

Since further information to better understand Internet banking in Malaysia is needed, this research investigates the risk, trust and security effect, consumer's intention to use Internet banking. The following are the objectives of this study:

1. To investigate the influence of Quality on Perceived Usefulness towards the Intention to continue using Internet banking.
2. To investigate the influence of Risk dimensions on the Attitude towards the use of Internet banking.
3. To investigate the influence of Perceived Ease of Use on the Attitude towards the use of Internet banking.
4. To investigate the influence of Perceived Usefulness on the Attitude towards the use of Internet banking.

5. To investigate the influence of Perceived Privacy on customers‟ Trust in Internet banking.
6. To investigate the relationship between each of the security requirement factors (Authentication, Confidentiality, Data Integrity and Non-repudiation) and Trust towards intention to continue using Internet banking.
7. To investigate whether Perceived Trustworthiness moderates the relationship between privacy, security and trust.
8. To investigate whether Perceived Effectiveness of Biometrics Technology Usage moderates the relationship between security and trust.
9. To investigate the influence of Trust on Intention to continue using Internet banking.
10. To investigate the influence of customers‟ Trust in Internet banking on Attitude towards the use of Internet banking.
11. To investigate the influence of Attitude towards the use of Internet banking on Intention to continue using Internet banking.

1.5 Research Questions

According to the Research Objective 1 to 11, research questions were advanced accordingly as follow:

1. Does Quality influence Perceived Usefulness?
2. Does the Risk dimension influence the Attitude towards Intention to continue use Internet banking?

3. Does Perceived Ease of Use influence the Attitude towards intention to continue use Internet banking?
4. Does Perceived Usefulness influence the Attitude towards intention to continue use Internet banking?
5. Does Perceived Privacy influence Trust?
6. What is the relationship between each of the security requirement factors and intention to continue use Internet banking?
7. Does Perceived Trustworthiness moderate the relationship between privacy, security and trust?
8. Does Perceived Effectiveness of Biometrics Technology Usage moderate the relationship between security and trust?
9. Does Trust influence Intention to continue use Internet banking?
10. Does Trust influence Attitude towards intention to continue use Internet banking?
11. Does Attitude influence towards Intention to continue use Internet banking?

1.6 Significance of the Study

This study is expected to contribute to both theoretical and practical perspectives. There are several reasons why this study is important. First, the topic represents three research streams that are risk factors, trust, and security dimensions towards intention to continue using Internet banking.

Internet banking will be compared by customers with other methods of banking to weigh if perceived benefits outweigh the perceived risks and costs. In

addition, the decision to continue using will be considerably influenced by the availability of sufficient assistance, the competence and knowledge of banking providers. The progress and execution of a sound security system is required in Internet banking as it is a financial service in electronic commerce that is continually growing. Hence, effective methods need to be designed for the possibility of authentication in a remote environment. A unique way to identify and validate users without the authenticity method ever being cloned is definitely an element that is needed for Internet banking applications.

By just reading the signals, following the trends and issues on security would not be everything for Internet banking. Internet banking crimes keep increasing by the day. Thus, the findings from this research could provide important suggestions as to the extent of enhancement that could be done at the level of security in Internet banking. The cyber crimes such as phishing activities keep increasing every quarter. Security issues could be enhanced by investigating biometric authentication systems in online banking; this could secure the login process to the system; password vulnerabilities could be removed; convenience could be enhanced whereby users could login with their finger quickly; and help desk expenses would reduce due to elimination of password resets based calls.

As significant contributions to the research in Internet banking is the enhancement of security issues biometrics implementation suggestion. Biometrics is not a new thing in the market. Fingerprint is one form of biometric implementation which has been used since 100 year ago for criminal purposes. In Malaysia, biometrics has been used in e-government environment and the largest department that used the biometrics technologies was National registration department. Looking

at the trends, foreign bank such as HSBC Bank in Malaysia has introduced a second level of security for their Internet banking which is log-in, password and USB device. However, still some problems would crop up when customers forget to bring the USB device or when they lose the device. This solution still limits them to access Internet banking services. The proposed solution using biometrics will help to reduce the security issue and safety solution to the Internet banking users. Significance in terms of contribution to banking perspective it may leads to increase profit since the issue of fraud can be control. This is due to the authentication using biometrics may help to enhance the level of unauthorized activities. Besides that, it will reduce losses in operation and financial factors. In terms of contribution to the government, it will secure the e-government network especially due to the financial activities. The confidence and trust level to the government will be higher since the issue of the security in financial institution is strongly protected with biometrics solutions. The e-government databases will be more secure by implementing this solution.

Therefore, implementation of biometric technologies to enhance the security level other than the normal authentication (login and password) would be the best solution and unique security solution. This is a new technology adoption in Internet banking, even though this system has been used in other authentication such as in immigration, airport gate, e-government, e-commerce, and so forth. There is the possibility that biometrics technologies could be implemented in the Internet banking environment, using say, fingerprint, iris, keystroke, speech, and so forth. The combination of these factors such as fingerprint with the speech, or iris with the fingerprint would be the best solution. Fingerprint scanner via USB has been