THREATS AND THE EXISTENCE OF SECURITY CONTROL PROCEDURES IN COMPUTERIZED BANKING SYSTEM: EVIDANCE FROM MALAYSIA

BY

ABUBAKAR MALAMI

A dissertation submitted in fulfilment of the requirement for the degree of Master of Science in Accounting

Kulliyyah of Economics and
Management Sciences

International Islamic University
Malaysia

JULY 2012

ABSTRACT

The rapid development and use of technology in the dissemination of information has embraced new dimensions among individuals, organizations, and government establishments. The banking industry is not an exception. As service orientated institutions, banks need information in executing their business activities. The proliferation of innovative-technological services by banks - use of mobile banking, e-transfer funds, internet banking, automated teller machine (ATM) among others- resulted into the increased use of sophisticated technologies in disseminating information or to information system (IS). Given that no system can be made absolutely secure, executing adequate security controls over organizations' information systems and other organizations' assets become necessary. It is against this background that this study attempted to examine threats and the existence security control procedures in the Malaysian computerized banking system (MCBS). The study specifically targeted banks operating in Kuala Lumpur. Data was collected through postal mail questionnaires. The findings show that the respondents perceived the likelihood prevalence of threats in their respective banks in a range of areas. It also revealed that there is significant difference among the Malaysian computerized banks' branches regarding the extent of security control implementation in control activities, risks assessment and monitoring control procedures. However, the results on the existence of threats show non-significance difference in all the threats variables. Moreover, the study found that there is reasonable level of security control implementation in the observed banks' branches. Therefore, the research concluded that there were adequate rate of implementation of security control procedures in the Malaysian computerized banking system. Moreover, the study suggested that the banks should consider continuous improvement in some of their security control procedures.

خلاصة البحث

عبي الرغم من التطور السريع واستخدام تقنيات نشر المعلومات قد بلغ مجالات جديدة عند الأفراد والنمظمات والمؤسسات الحكومية بكافة أشكالها واحجامها, فإن القطاع المصرفي لايعتبر استثناءً في هذا المجال. تعتبر البنوك مؤسسات خدمية بحاجة معلومات لتنفيذ نشاطاتها المالية. إن تطوير وسائل التقنية الجديدة من قبل البنوك باستخدام وسائل الجوال المصرفي, تحويل المبالغ الكترونيا, الخدمات المصرفية عبر الانترنت, والصرافات الآلية, أدى إلى ازدياد استخدام التقنيات المعقدة لنشر المعلومات والتي أصبحت حالياً أنظمة معلومات مؤتمتة. وباعتبار أنه لايمكن إجراء تأمين مطلق لأي نظام, لذا فإن إضافة إجراءات أمان إضافية على أنظمة معلومات المنظمات وأصولها أصبح ضرورياً. وعلى هذا فإن الدراسة الحالية كانت بخصوص إدارك مدراء البنوك للتهديدات الامنية الإجراءات الأمنية الحالية في نظام المعلومات الماليزي المؤتمت في كوالالامبور. تم جمع معلومات هذا البحث من خلال استبيان مرسل بريدياً مصمم خصيصاً لتلبية أهداف البحث. أظهرت نتائج الحث أن المدراء المستجيبين لديهم تصور عن احتمال تهديدات لبنوكهم. أظهرت النتائج أيضاً أنه لايوجد احتلاف ملحوظ بين مختلف البنوك فيما يتعلق بمدى تنفيذ إجراءات الأمان. في حين أظهرت الدراسة وجود مستويات عالية من إجراءات الأمان في فروع البنوك التي شملتها الدراسة. وعلى هذا الاساس, يمكن الاستنتاج بوجود تنفيذ متكرر لإجراءات الأمان في النظام المصرفي الماليزي المؤتمت. بالإضافة تقترح الدراسة أن ابنوك يجب أن تأخذ بعين الاعتبار تحسين الإجراءات الأمنية لديهم.

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 research paper for the degree of Master of Science in Accounting.

…………..……………………………
Zaini Zainol
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 research paper for the degree of Master of Science in Accounting.

…………..……………………………
Ahmad Zamri Hussain
Examiner

This dissertation was submitted to the Department of Accounting and is accepted as a fulfilment of the requirement for the degree of Master of Science in Accounting.

…………..……………………………
Hafiz-Majdi Ab Rashid
Head, Department of Accounting

This dissertation was submitted to the Kulliyyah of Economics and Management Sciences and is accepted as a fulfilment of the requirement for the degree of Master of Science in Accounting.

…………..……………………………
Khaliq Ahmad
Dean, Kulliyyah of Economics and
Management Sciences

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.

Abubakar Malami

Signature……………………….. Date…………………………..

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

THREATS AND THE EXISTENCE OF SECURITY CONTROL PROCEDURES IN COMPUTERIZED BANKING SYSTEM: EVIDANCE FROM 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 Abubakar Malami

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

I dedicate this research work to my parents, who always supported me in every endeavor. They are the reason I'm here at all, and made me who I am today.

ACKNOWLEDGEMENTS

In the name of Allah the Most Gracious and the Most Merciful

Alhamdulillah, all praises to Allah for the strengths and His blessing in completing this research work. Also praise is only to Allah the Almighty for his bounty and blessing showers upon us and peace upon our prophet Muhammad (S.A.W) his family, his companions, and those who follow his teaching until the end of the day.

My special and sincere appreciation goes to my supervisor, Dr. Zaini Zainol, for his supervision, continuous support and encouragement. His invaluable help of constructive comments and suggestions throughout the preparation of this thesis have contributed to the success of this research

My deepest gratitude goes to my beloved parents; Alhaji Malami Ibrahim and Mrs. L. Ahmad and also to my brothers, Arsana Shehu Isma'il Malami Abdurrashid Umar, Uwaisu Malami and my lovely sisters Saratu and Aisha for their endless love, prayers and encouragement. Not forgetting my fiancé, Herleemath Malami for her love and care.

Last but not least, my sincere thanks to all my friends especially Doc. M.M. Bello, Sulaiman Umar, Sa'adu Sidi, Abdullahi Sidi among others for their kindness and moral support during my study. Thanks for the friendship and memories. To those who indirectly contributed in the completion of this research work, your kindness means a lot to me. Thank you very much.

Abubakar Malami 2012

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

AICPA	American Institute of Certified Public Accountant
AIS	Accounting Information System
AISS	Accounting Information System Security
CAIS	Computerized Accounting Information System
CBS	Computerized Banking System
CEOs	Chef Executive Officers
CIOs	Chief Information Officers
CICA	Canadian Institute of Chartered Accountant
COBIT	Control Objectives of Information & Related Technology
COSO	Committee of Sponsoring Organizations of the Treadway
EBI	Egyptian Banking Industry
ICT	Information & Communication Technology
IS	Information System
ISACA	Information System Audit & Control Association
ISG	Information Security Governance
ISO	International Organization for Standardization
IT	Information Technology
ITG	Information Technology Governance
ITGI	Information Technology & Governance Institutions
MCBS	Malaysian Computerized Banking System
SANS	SysAdmin Audit Networking and Security
SAC	System Audibility and Control
SBS	Saudi Banking Sector
SYSTRUST	System Trust

CHAPTER ONE

INTRODUCTION

1.0 INTRODUCTION

This chapter discusses the background of the research topic: threats and the existence of security control procedures in Malaysian computerized banking system. This is followed by brief discussion of the research problem, the objectives, research questions, motivations, contributions and the organizations of the research chapters.

1.1 BACKGROUND OF THE STUDY

With the advent and expansion of information and communication technology (ICT), and with the coming of globalization (i.e. competitive and/or information age), the use of computer and other electronic devices had improved (Walters, 2007). Consequently, the mode of operations in different sectors of our communities has been developed. As such the establishment of information system has been obvious in the banking industry. Banks try to put in place computerized systems that will ease their daily operations (Fowzia and Nasrin, 2011). The information system has become the life blood of modern organizations and it has become the heart of today's modern banking system (Musa, 2004).

Subsequently, the traditional ambit of banking operation has taken a new length; this necessity is due to the large number of transactions being processed by the banks as well as attainment of competitive advantage. As a result of these transactions on a daily basis, the use of computers and other related devices such as the Internet has become inevitable. The use of these devices by both the bank and its customers has eased the transaction process between the parties, to the extent that customers can directly communicate with their banks to perform various transactions. For example, payment of bills, transfer of funds, balance inquiry, and other such services offered by the banks.

Basically, information technology creates value to the organizations. For instance, through increasing revenues at marginal cost, reduction of expenses and thus, enhancing operating profits (Mashhour and Zaatreh, 2008). Similarly, it provides accurate and reliable information at a high speed. However, organizations should not only take note of its efficiency. But also take the cognizance of its negative implications, which in many ways deter their achievements. Innovation in information technology (IT) has raised concerns about the risks to data associated with IT security, including vulnerability to viruses, malware, attacks and compromise of network systems and services (Lallmahamood, 2007). Similarly, Mansour et al. (2009) highlighted that inadequate IT security may result in compromised confidentiality, integrity, and availability of the data due to unauthorized access.

Information security risks had been a major problem to the operations of information system, particularly in the computerized banking system, due to the fact that IT based organizations were more concerned with information in dealing with their clients (Martin, 2005). As banks and other institutions began to embrace computerization in their institutions, only few knew that they were setting the pace in cyber-crimes era (Martin, 2005). This could be the result of total adoption of computers and technological devices that are user-friendly such as; the Internet, laptops, and now smartphones, by individuals and corporate bodies of all types and sizes.

As a result, securing information system resources from dishonest and deceitful groups of individuals is of utmost important (Musa, 2006). It is quite noticeable today that cyber fraudulent activities are not only executed by ordinary people, but with the professionals in the field; this brings a new sort of white collar criminals that can easily penetrate organizational confidential information (Loch et al., 1992; Ula et al., 2011). As such absolute protection of information system became difficult and more complicated (Whiteman, 2004).

However, Musa (2006) highlighted that business survival and success are heavily dependent upon the accuracy, integrity and continued availability of reliable information. Moreover, Gupta and Hammond (2005) also emphasized that for organizations to have efficient and effective information systems, there must be adequate, accurate and appropriate, timely dissemination of information within their system. These must be in line with the organizational goals and strategies to maintain the process and disseminate information that can be used for decision making by different stakeholders of the organization (Gupta and Hammond, 2005). In order for an organization to gain competitive advantage, modern information technology infrastructure, as well as adequate security controls must be in place.

According to Hayale and Kadrah (2006) computerized banking systems may encounter serious security threats as a result of a weakness in their internal control systems or from the nature of the competitive environment (i.e. information age). Failure to secure the information assets might lead to greater losses of financial and non-financial assets of an organization (Musa, 2010). It was observed that institutions that gave less attention to potential security threats were more likely to encounter serious challenges with their information security controls (Musa, 2006). Consequently, many organizations are compelled to device a comprehensive security controls system to protect their information assets against security threats (Sun et al., 2006).

In view of this, organizations' management must be abreast with the technological and security risk advancement. This is because the more they are aware of the threats and frauds confronting their organizations' information systems, the better they can assess, analyze risk, and implement appropriate controls to protect the organizational assets. In response to this, organizations are now giving particular attention to their information security control system in the light of computer hackers, fraud, insiders and computer viruses. Understanding and employing adequate security control measures over their information systems has become an issue that no business can ignore (KPMG, 2000; Musa, 2004; Gupta and Hammond, 2005). Therefore, this study seeks to explore the threats and the occurrence level of security control procedures among banks' branches in Malaysian computerized banking system (CBS).

1.2 RESEARCH PROBLEM

The advent of information technology has considerably changed almost all the organizational operations globally (Fawzia and Nasrin, 2010). One response to this change is the development of accounting programs that lay emphasis on the development of accounting information systems (Fawzia and Nasrin, 2010). This development has not only impacted on accounting operations in financial institutions but also touched many aspects of our lives (Gupta and Hammond, 2005). For instance, it is contributing tremendously to health, education, air traffics controls, stock exchange, and telecommunications. According to Gupta and Hammond (2005) the world is rapidly moving to the point where everything depends on software. However, the issues of information security control system and threats have become an issue that need to be considered for the successful implementation of a computerized banking system.

The introduction of information technology had made the accounting processes undergo major changes (Ula et al., 2011). Initially, accounting records are recorded, processed and reported manually. But with the advent of technological innovations in the development of computerized banking system (i.e. IT), the operations have changed to a more effective one, which has affected the way accounting records are being processed. In view of this, the control approach of accounting information would be different from that of hitherto, which has proposed new requirements towards a sound internal control system (Ula et al., 2011).

Gupta and Hammond (2005) highlighted that technological innovations usually increase efficiency and ability to instantly connect on a global scale. As a result, the danger of risks becomes more sophisticated and difficult to contain. Similarly, there are daily reports in accounting and financial publications regarding computer related data errors, incorrect financial information, violation of internal controls, thefts, burglaries, fires and sabotage (Strong et al., 2006). Though efforts have been made by auditors, managers, accountants and information specialist to reduce vulnerability to such events, yet increased effort is still required (Strong et al., 2006). Consequently these may lead to the loss of computer assets, increased risk of fraud, competitive disadvantages, loss or theft of data, privacy violations, and business disruption of computerized banking system (Khan and Barua, 2009). In view of the development of information system, banking operations have some levels of insecurity that could lead to risk (Musa, 2006).

Therefore, organizations need to critically evaluate and understand the major threats confronting their computerized system, so that they could device appropriate control measures against such threats. In this regard, the internal control of the information system becomes the primary concern in the internal control of the banks so as to conduct effective operations and maximize efficiency, which in effect means overcoming business operational risks and computer crimes.

The current study seeks to investigate and find out threats and the existence level of security control procedures in the Malaysian computerized banking system. This is because businesses today are faced with far greater challenges than before, due to economic, technological and legal interdependence and interconnectedness (Chaffey and wood, 2005). It is useful to find out more about the threats that affect the operations of computerized banking in Malaysia. With an attempt to also explore the security control procedures that are in place and how those control measures facilitate the smooth running of the banking sector in achieving the banks' IT objectives in respect to threat identification and mitigation.

1.3 OBJECTIVES OF THE STUDY

The main purpose of this study is to investigate threats and the existing control procedures in computerized banking system in Malaysian banks' branches, by studying the opinions of the bank managers of conventional banks, conventional bank with Islamic window and Islamic banks. The current study has the following objectives:

1. To determine the major threats that are likely to challenge computerized banking system in Malaysia.
2. To determine whether threats differ significantly among the type of banks' branches in Malaysian computerized banking system.
3. To determine whether the practices of control in Malaysian computerized banking system differs significantly among the types of bank branches.

1.4 THE RESEARCH QUESTIONS

The current study seeks to bring light to the vulnerabilities of threats, the extent of control procedures in the Malaysian computerized banking system. The current study is a replication and extension of the work of Musa (2006 and 2004) with some modifications. The study explored and employed the following research questions:

1. What are the major security threats that are likely to face computerized banking system in Malaysia?
2. Is there significant difference in threats among the types of banks' branches in Malaysian computerized banking system?
3. Is there significant difference in practices of control in Malaysian computerized banking system among the types of banks' branches?

1.5 SIGNIFICANCE OF THE STUDY

This study is significant; as its findings may help managers, accountants, auditors, information specialists, within financial institutions to fully understand the implications of threats against their security control systems (Musa, 2004; 2006; Hayale and Khadra, 2006; 2008). It is hoped that the findings of the study would help the computerized banks in Malaysia to design and formulate a sound and effective security control system that will provide reasonable assurance for the accomplishment of the institutions' mission. The research is expected to provide a platform for the regulatory authorities to appreciate the impact of their activities on an organization, and underscore areas for improvement. Moreover, the findings of the current study are expected to contribute not only to the computerized banking institutions, but also to financial institutions in general or those organizations that have similar nature of operations with the banks under study.

Additionally, the research is relevant in understanding the concept of internal control system, threats and information system security. It is worth mentioning that the present state of the global information security faces serious challenge that needs to be addressed (Strong et al., 2006). Hence, this study attempts to examine the threats and the existence of security control procedures in the Malaysian computerized banking system. As part of its contribution, this research work is projected to benefit the academic community. Since, other researchers may reference it to investigate further issues on the subject of study.

1.6 MOTIVATION OF THE STUDY

The motivation of this research is of threefold. Firstly, the researcher was motivated to conduct the research as a result of limited literature on the subject of study (i.e. threats, internal control security system in computerized banking) in the context of developing nations (Musa, 2004; 2006; Hayale and Khadri, 2006). Undertaking this research will help in bridging the gap in the existing literature. The researcher was also motivated by the frequent number of cases of cyber fraud and crime cases that were being recounted in accounting and financial publications as well as in local magazines (Strong et al., 2006). The researcher attributed this to weak internal control security system in place (Hayale and Khadra, 2006). Though, researches have been conducted on corporate governance and corporate reporting in the banking sector, conducting a research of this nature would contribute in addressing the literature gap regarding information security control, specifically in the context of banking industry.

1.7 ORGANIZATION OF THE STUDY

The present chapter gives a brief background of the study and also explains the purpose for which the study is being conducted. It outlines the research objectives, questions and contribution of the research. In the next chapter, a general discussion of the nature of internal control system, threats and information security system is presented. This discussion is from the review of some previous studies. This is then followed by chapter three which discusses the theoretical framework, hypotheses developed as well as the research framework. While the methodology used in the research is deliberated in chapter four. It includes research design, population and sample size of the study, development of the instrument, processes of data collection and the location in which the research was conducted. Finally, the chapter discloses data analysis techniques employed in the study. Data analysis, discussion and interpretation of the results are presented in chapter five. Finally, chapter six delivers key findings and recommendations. It also provides a discussion on the limitations of the study and it finally finishes with future research suggestions.

1.8 CONCLUSION

The current study provides literature on information threats and security controls in a computerized banking context, and it complements previous studies regarding the issue of security practices. However, this chapter presents the research problem; it