SECURITY THREATS OF COMPUTERIZED BANKING SYSTEMS (CBS): THE MANAGERS' PERCEPTION IN MALAYSIA

Abu Bakar Malami
International Islamic University Malaysia
Researcher
E-mail: amalams2008@yahoo.com

Zaini Zainol
International Islamic University Malaysia
Senior Lecturer
E-mail: zzaini@iium.edu.my

Sherliza Puat Nelson
International Islamic University Malaysia
Senior Lecturer
E-mail: sherliza@iium.edu.my

—Abstract —

Internal control system is an important pillar in an organisation. Considering the evidence from major accounting fraud cases that occurred consequence to weak internal control, such as Enron, it could also occur in a financial institution. Hence, the objective of this study is to investigate the bank managers' opinion on the likelihood of security threats in the computerised banking systems (CBS) in Malaysia. Since most major financial institutions operate in the capital city of Kuala Lumpur, questionnaires were sent to selected bank branches in Kuala Lumpur. The findings are expected to provide a platform for bank managers to share their threats' experience. Secondly, to assist them in designing and formulating a sound and effective internal control system that will provide reasonable assurance for achieving the bank's mission. Findings are also expected to provide general insights of internal control system, as most information is very remote and confidential, thus generate a platform for promoting an efficient and effective internal control practice in financial institutions.

Key Words: *Threats, Internal Control, CBS, Malaysia*

JEL Classification: M15, M41, M40

1. INTRODUCTION

The increase use and the surge reliance on technological facilities by individuals, corporations, and governments in performing an effective and efficient operation of their daily business activities (Davis, 2001), had change the length of information dissemination, more especially in the IT based organization. Consequently, the risk to ensure adequate security of information system has significantly increased (Musa, 2006a). Jackson (2000) highlighted that loss of information or a breach of security could be financially devastating. Similarly, Jin and Cheng (2005) contended that loss of confidential data or the destruction of information assets would financially harms organizational reputation. The growth use of the Internet by IT based institutions has heightened the threat of cyber-crimes, and also it evolved a medium for some people to commit other computer related crimes. According to the National Institute of Standards and Technology (2005) IT based organization are more vulnerable to various threats which could directly or indirectly cause various types of damages that may cause a substantial financial loss. These damages may range from human based threats, technological based threats, and natural and/or environmental threats.

The implication of these threats would adversely implicate an organizational database integrity that may cause destruction of the entire organizational database. In view of this, there is need for organizations to carefully and cautiously explore and understand the major threats facing their information system, so that, appropriate security control measures should be properly devised against information security risk. The objective of the paper are; (1) to offer discussion on the potential threats in computerized banking systems by reviewing literature; (2) to investigate the threats that likely to face the Malaysian's computerized banking system.

The structure of this paper is organized as follows. The next section discusses the review of related literature regarding the issue of information system security threats, followed by the methodology applied in this study, while the next section demonstrates the empirical findings as well as the discussion of the research. Finally, the paper concludes by proposing some recommendations.

2. LITERATURE REVIEW

Statistic shows that financial institutions play a vital role to the growth of global economic activities (Casolaro and Gobbi, 2004). According to Treasury Malaysia, industries within the Malaysian service sector (i.e. financial & insurance industries) played a pivotal role to the Malaysian service GDP in 2008, in which

the finance and insurance services, accounted for 21 percent of the GDP.[1] Also, Bank Negara Malaysia (BNM) in its 2010 Annual Report demonstrated that the sector has the largest contribution to the Malaysian economic growth contributing 3.9 percentage points to the overall GDP growth[2]. As such the sector has to be given due consideration that would help it improves its performance.

The rapid change in information technology, the wide spread of user-friendly devices and the dependence of organizations on information system to execute their various operations have increased various threats to information system security which in turn adversely affect the business operation (Chang and Jan, 2010; Musa, 2006a, 2010; Sun et al., 2006; Kankanhalli et al., 2003; Salehi et al., 2010). Specifically, the growing dependent on the computerized information systems by banking and financial sector in executing its business operations have made it impossible to separate information technology (IT) from the business of the banks and the financial institutions (Beheshti, 2004). Thus, the need for focused attention on the issues of the information systems security risk in computerized system and the security controls to safeguard information and information systems (Musa, 2004).

Empirically, Loch et al. (1992) conducted a study on threats to information security. The findings of their study revealed that unintentional human based threats, natural disaster threats and technological based threats were ranked among the major threats challenging Egyptian banking industry. In replication of the work of Loch et al., (1992) Davis (1996) study revealed that employees' entry of bad data and the accidental destruction of data as well as the computer viruses were considered to be the most threats in a microcomputer environment. However, unauthorized access to data and /or system by employees' accidental entry of bad data by employees and poor segregation of duties were rated as the major threats to the mid-range computer environment. Musa (2006a) investigated and evaluated the existence and adequacy of implemented accounting information system security control in the Saudi organizations in order to prevent, detect, and control accounting information system security breaches. He found out that there were adequate implementations of controls to the Saudi organizations' accounting information system security. Similarly, Musa (2006b) investigate the perceived security threats to computerized accounting information system in the Egyptian banking industry by surveying the entire population of the EBI. His study revealed that accidental entry of bad data by employees, introduction of computer

[1] Treasury Malaysia, Economic Report 2009/2010, 2009
[2] Bank Negara Malaysia Annual report 2010 (http//www.tindakmalaysia.com)

viruses to the system, natural and human made disasters, employees sharing of passwords, misdirecting of prints and distribution of information to unauthorized people were found the most significant perceived security threats to CAIS in the EBI.

3. RESEARCH METHODOLOGY

The current study is empirical by nature; the data of this study were collected using a postal self-administered questionnaire. The questionnaires have been distributed to the selected 201 banks branches operating in Kuala Lumpur, Malaysia. The questionnaire was adapted from the work of (Musa, 2006b). The respondents were asked to indicate the degree of occurrences of each security threats by indicating one among the five available options: that range from 'Not likely to occur' to 'most likely to occur'.

Cross-tabulation statistics of the collected data were designed to gain better understanding of the research variables. Out of 201 questionnaires distributed to target respondents (i.e. Bank Branch Managers) only seventy six were returned representing 38.0% of the response rate. We divided type of threats into five categories namely human threats-unintentional, human threats-intentional, technological threats, natural threats, and environmental threats (www.sans.org/).

4. RESULTS AND DISCUSSION

4.1 Respondent profile

Table 1 indicates different types of bank branches considered in the study. The results show that conventional bank has the highest rate of percentage with 78.9% (60) whereas Islamic bank has frequency of 16 indicating 21.1% of the total branches. In term of working experience, 40 (52.6%) of the respondents stated that they were working in their current position for more than ten years. While 36 (47.4%) of the respondents reported to have less than ten years' working experience in the observed bank branches. From the statistic, it could be inferred that since the majority of the respondents were in their current positions for more than ten years, they were expected to have capability, skills and knowledge about their jobs, and thus, that may increase the accuracy and reliability of their responses.

Table 1
Respondent Profile

Items		n	Percentage
Type of Bank	Conventional Bank	60	78.9%
	Islamic Bank	16	21.1%
	Total	76	100.0%
Working experience	> 10 years	40	52.6%
	< 10 years	36	47.4%
	Total	76	100.0%

4.2 Perception of threats

This section provides a discussion regarding their perceptions of the likelihood of threat occurrences in their respective banks' branches. Each of the respondents were asked to indicate his/her opinion by chosen from the available options (i.e. from 'Not-likely' to 'Most-likely'). Table 2 shows the bank managers' perception on the likelihood of threats to occur in their computerized banking system.

Table 2
The Likelihood of Threat

Type of threats	N	Not likely	Least likely	Likely	Very likely	Most likely
Human Unintentional Threats	76	18.4%	14.5%	23.7%	34.2%	9.2%
Human Intentional Threats	76	19.7%	19.7%	28.9%	23.7%	7.9%
Technology Based Threats	76	19.7%	23.7%	25.0%	26.3%	5.3%
Natural Threats	76	40.8%	26.3%	11.8%	19.7%	1.3%
Environmental threats	76	18.4%	28.9%	26.3%	19.7%	6.6%

4.2.1 Human Unintentional Threats

This variable attempted to determine how banks' branch manager perceived the possibility of human accidental threats in their banks. As human being is the engine of an organization be it IT based or not, they are considered to be one of the threats to the banks. Table 2 shows the rates of accidental human threats among the respondents from different types of banks' branches. The results revealed that majority of the respondents from all the banks' branches alleged that their banks were very likely to have faced unintentional human threats with 26 (34.2%), which constituted approximately one-third of the respondents. Also, 18 (23.7%) believed that their banks were likely to confront this type of threats. However, 14 (18.4%) and 11 (14.5%) responded that their banks' branches were not likely or least likely to face such threats respectively.

In light of this, it could be said that all the three banks' branches were confronted with this type of threats. This might be the result of lack of technical and/or adequate knowledge among the employees to operate the system. To mitigate the likelihood of this threat; continual training of employees should be scheduled and computer system and/or robot system should be put in place to substitute human services. Prior studies (Loch et al., 1992; Neumann, 1995; Baskerville, 1996; Cohen, 1997) confirmed that human unintentional threats were the most significant threats against the information system. However, Paul and Baskerville (2005) longitudinal study of information system threat contradicted prior studies that human unintentional errors were the major threats to information system. Their results indicated that the threats appeared to be insignificant and a poorly recognized issue for information systems security. The result of their study was also inconsistent with this current study as the findings of this current study indicated high level of the likelihood of this threat.

4.2.2 Human Intentional Threats

This variable starts to explore the view of banks' managers on the likelihood of intentional threats. Deliberate human threats is one of the major threats that challenging institutions, as there were disgruntle employees, hackers among other, that deliberately stole an organization's resources for their personal uses. The research findings depicted that a total of 15 respondents (19.7%) reported that their banks did not encounter any of this type of threats as shown in Table 2. A similar number of respondents supported this view when they said that their banks were less likely to have faced this threat. However, a relatively large percentage (28.9%) of respondents declared that they were likely challenged by this kind of threats in their bank branches. Thus, 18 (23.7%) believed that their banks were very likely to have faced the threat. With few respondents representing (7.9%) declared that they were most likely to be attacked by the threat. Overall, the banks' branches were somewhat challenged with this threat, most of the respondents were of the belief that they were likely or even very likely to face this type of threat. In this regard, the banks should reconsider reviewing their management philosophy and style. More especially, when it comes to training of employees thereby intensifying staffs knowledge and skills that would help reduce the occurrences of accidental errors. Similarly, recruitment policies and procedures such as background check of employees to avoid employing dishonest or untruthful personnel in the banks.

4.2.3 Technology Based Threats

Development and rapid adoption of technology by institutions have increased technological threats, especially in the IT based organizations such as banks. Therefore, this variable attempted to determine the likely occurrences of this threat in the Malaysian computerized banking system.

Technological threats are inevitable in almost every organization. More especially the IT based organizations (e.g. Banks), the results demonstrated that 19 (25.0%) and 20 (26.3%) of the respondents reported that they were likely and very likely to have confronted with technological threat in their respective banks (Table 2). However, nearly similar percentages of respondents were of the opinion that they were not or least likely to encounter with the threat, with approximately 19.7% and 23.7% respectively. While only few of them declared that they were seriously faced with the threat. Moreover, the overall findings revealed that the banks were more or less challenged by the technological threat. This result therefore suggests that banks should upgrade their security software infrastructures with the latest technology facilities such as the latest antivirus, and sophisticated control network, etc.

4.2.4 Natural Threats

Natural threats variable attempt to determine the degree to which banks' branch managers perceived the likelihood of the natural threats through wild fire, floods and so on. Table 2 shows cross tabulation of the natural threats by the respondents among different types of banks' branches. The results show that relatively high proportion of the respondents (40.8%) confirmed that their banks were not likely to face with natural threats. More than quarter or one-fourth (20 or 26.3%) of them affirmed that they were least likely to be confronted with this type of threat. Fifteen respondents believed that they were very likely to have faced with natural threat, while approximately 12% were of the view that they were likely to have encountered the threat. Only one respondent declared that his bank branch seriously confronted with natural threat. Exclusively, it could be observed that the banks were not or at least likely to have this kind of threat. Moreover, Malaysian territory is not prone to natural disasters such as earthquake, floods, wind disasters wildfire etc., and in particular the bank branches location were also not subject to this threats as they were on high ground areas.

4.2.5 Environmental threats

The statistical findings of Table 5.8 show the response rate of the environmental threats among different types of banks' branches. Almost one third of the

respondents 29.0% revealed that their banks were least likely to encounter environmental threat. Similarly, nearly the same percentage of the respondents (27.0%) indicated that their banks were likely to face with the threat. About 19.7% reported that their banks' branches were very likely to be confronted by this threat. However, 14 (18.4%) were of the view that their banks were not likely to have faced this kind of threat. 5 respondents reported that they believed that they this threat was a challenge.

5. CONCLUSION

Based on the above analysis, the findings regarding the level of the likelihood of threats in the CBS in Malaysia revealed that the major threats challenging the CBS in Malaysia in the ranking order were; 1- Human unintentional threats, 2- Human intentional; 3- Technological threats; 4- Environmental threats and the last one was 5- Natural threats. The findings were able to answer the first research question as; 'what is the major security threats facing computerized banking system in Malaysia'? The result was coherent with the previous studies reported human errors as the top-ranked security threats (Loch et al., 1992; Whitman, 2004). It was evidently investigated that human errors are unavoidable (Whitman, 2004). The two surveys piloted the reasons of failures, due to operators, hardware failures, software failures, and overload (Wood, 2000).

Moreover, the findings also indicated that on average the respondents perceived the likelihood of threats occurrences on a scale of 'likely' in their banks. This finding is consistent with the prior studies (Loch et al., 1992; Cohen, 1997; Baskerville, 1996; Musa, 2004, 2010). In view of this, banks' branches should consider strategizing their security control procedures or policies in combating the likelihood or occurrences of these threats. Wood (2000) emphasized that security system should begin with valid security policy; the policy is then translated into action through an effective security strategy that focuses on the prevention, detection, and correction of threats. Furthermore, employees' education, knowledge, and skills relating to information security system should be regularly and adequately improved, so that unnecessary errors within the banks would not occur. Therefore, for the banks to remain competitive and improve their information security system appropriate and effective control measure should be devised within their information security system.

REFERENCES

Abu-Musa, Ahmad A. (2006b), "Exploring Perceived Threats of CAIS in Developing Countries: The Case of Saudi Arabia", *Managerial Auditing Journal*, UK, Vol. 21, No. 4, pp. 487- 407.

Abu-Musa, Ahmad A. (2006a), "Evaluating the Security Controls of CAIS in Saudi organizations: The Case of Saudi Arabia", *The International Journal of Digital Accounting Research.,* Vol. 6, No. 11, pp. 25- 64.

Bierstaker, J. L; R. G. Brody; and C. Pacini, (2006) "Accountants' Perceptions Regarding Fraud Detection and Prevention Methods" *Managerial Auditing Journal, UK*, Vol. 21, No. 5, pp. 520 -535.

Casolaro, L. and Gobbi, G. (2004). Information technology and productivity changes in the Italian banking industry. *Report Published by Bank of Italy Economic Research Department,* pp. 1-26

Chang S. and Jan D. (2010). SOX 404-compliant ERP system internal control framework: The preliminary outcome. *Business and policy research*, pp. 282 – 295.

Davis C. E. (1996). Perceived security threats to today's accounting information system: A survey of CISA, *Information system audit control journal,* Vol. 3, pp. 38-41

Gupta A. and Hammond R. (2005). Information systems security issues and decisions for small and business: An empirical examination. *Information management & computer security,* Vol. 13, No. 2, pp. 297-310.

Jackson C., (2000) "Discussion of Information Technology-Related Activities of Internal Auditors", *Journal of Information Systems*, Vol. 14, No. 1, pp. 55-56.

Kankanhalli, A., Teo, H., Tan, B. and Wei, K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, Vol. 23, No. 2, pp.139-148

Kreicberg L. (2010). Internal threats to information security; countermeasures and human factor within SME. Master's thesis, *Lulea University of technology*

Loch, Karen D., Houston H. Carr and Merrill E. Warkentin (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, pp. 173 - 186.

Salehi M., (2010). Usefulness of accounting information system in emerging economy: Empirical evidence of Iran. *Economics and Finance,* Vol. 2, No. 2, pp. 186-195.

Strong, J. M., Portz K. and Busta B (2006). A First look at the accounting information systems emphasis at one University: An Exploratory Analysis. T*he Review of Business Information Systems*, Vol. 10, No. 2, pp. 235-256.