Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia - Social and Behavioral Sciences 65 (2012) 199 – 204

Procedia
Social and Behavioral Sciences

International Congress on Interdisciplinary Business and Social Science 2012

(ICIBSoS 2012)

Internal Human Based Threats and Security Controls in Computerized Banking Systems: Evidence from Malaysia

Zaini Zainol[a*], Sherliza Puat Nelson[b] and AbuBakar Malami[c]

[a,b,c]*Department of Accounting, Faculty of Economics and Management Sciences, International Islamic University Malaysia, P.O. Box 10, Kuala Lumpur, 50728, Malaysia*

Abstract

Malaysia being a unique capital market, practices dual banking system to capture the disaggregation of conventional and Islamic banking systems. However, like most financial institutions, no bank is isolated from security threats, even if, it comes from within the organization. Thus the objective of this study is to examine bank managers' experience on human based security threats and the existence of human based security controls in computerized banking systems (CBS) in Malaysia. Since most major financial institutions operate in the capital city of Kuala Lumpur, questionnaires were sent to some of these bank branches in Kuala Lumpur. Findings revealed that managers recognized the personal policies recruitment procedure, segregation of duties and physical access control as ways to mitigate risks of human security threats. Hence, provide insights of how internal control system of a financial institution can be improved as a means to reduce security threats that have monetary implications. Finally, the study provides a platform for promoting an efficient and effective internal control practices among financial institutions in Malaysia.

© 2012 The Authors. Published by Elsevier Ltd.
Selection and peer-review under responsibility of JIBES University, Jakarta

Keywords: human based threats; human based controls; Malaysia; computerized banking system

[*] Corresponding author. Tel.: +60361964670; Fax: +60361964609.
E-mail address: zzaini@iium.edu.my

1877-0428 © 2012 The Authors. Published by Elsevier Ltd.
Selection and peer-review under responsibility of JIBES University, Jakarta
doi:10.1016/j.sbspro.2012.11.111

1. Introduction

Information security risks have become one of the important areas in operating the information system of banks' highly sophisticated and computerized system. This is mainly because, information technology (IT) based organizations are more concerned with the information when dealing with their clients (Martin, 2005). The highly dependent on information technology, inevitably provides room for cybercrimes. As banks and other institutions continuously upgrade their computerized system, only few knew that they were setting the pace in cybercrimes era. The increase usage of computers and technological devices and gadgets that are user-friendly such as; laptops, ipods and smart phones; have open up areas for information exploitation and manipulation. Hence, securing of information assets from dishonest and deceitful groups of individuals is an utmost important for any financial institutions. Nowadays, the misused of technology is not only executed by ordinary people but also professionals. As such, white collar crimes among professionals have increased since these workers have greater access to the system (Loch et al., 1992; Ula et al., 2011). Accordingly, Whitman (2004) stressed that protecting information system from these workers was more difficult and complicated, as it came from within the organization.

Failure to secure the information assets might lead to greater loss of financial and non-financial assets of the organizations; it is believed that institutions that gave less attention to potential security threats were more likely to encounter serious challenges with their information security controls (Abu Musa, 2006). Understanding and employing adequate security control measures over their information systems is an issue that no business can ignore (KPMG, 2000; Abu Musa, 2004; Gupta and Hammond, 2005). Therefore, the objectives of this study are:

- To investigate human based threats and subsequently examine whether these human based threats existence differ from banks to banks branches in Malaysian computerized banking system.
- To examine whether human based security control systems implementation differs from bank to banks in Malaysian computerized banking system.

In the next section, we discuss some studies on security controls and threats in computerized banking system, research questions and hypotheses development.

2.0 Literature Review and Research Questions

2.1 Some Literature

The development of information technology indirectly gives a facelift to the business processes in banks, since this ensure efficient operations and improvement of communications within organizations and between the organizations and its customers (Liao et al., 2011). However, technology advances on the other hand, makes it difficult for organizations to secure their information resources, as the number of unauthorized persons gained accessed to information has increased drastically (Abu Musa, 2006). The nature of computer crime has changed over the years as a result of changes in technology. Subsequently, crimes were not only from IT jargons or professionals, but also from disgruntled employees who damaged the systems or stole information for revenge, or profit and monetary interest (Beheshti, 2004).

Bank as a service-oriented firm, needs information to deal with both it's existing and potential customers. Therefore, to remain in the competitive financial market, adoption of latest advances in information technology infrastructure is top priority for bank. Subsequently, keeping up-to-date with the recent changes and latest development in IT advances, is important in order to provide accurate and reliable information at an appropriate time (Khan and Barua, 2009). Mansour et al. (2010) discovered that Jordanian banking environment had acceptable rate of existence of principles and criteria such as

availability, security, maintainability, and integrity. Whilst Liao et al. (2011) studied the internal control system of the state-owned commercial bank computer system in China and found that internal control design of information system lacked hierarchy. This indicates that each level of the information system lacked the clear control goals and specific control measures.

2.2. Human Based Threats to Computerized Accounting System

Employees who have legal access to the organizational information, may intentionally or accidentally affect the organization's business activities (Walters, 2007). For example, trustworthy employees may cause problems to the information system by human carelessness, failure to follow established procedures, and poorly trained or supervised personnel; omissions; lost or misplaced data and logic errors etc. (Liu et al., 2009). In contrast, employees might also deliberately act to manipulate information assets due to some personal reasons. For instance, sabotage, computer fraud network based attacks, malicious software upload, unauthorized access to confidential information, embezzlement and so on (Walters, 2007; Dhillon and Torkzadeh, 2006; Liu et al., 2009). Hence, we propose the following research question:

RQ1: To what extent, do Malaysian Banks face human based threats (intentional and unintentional) in their computerized banking systems (CBS)?

Subsequently, we are also interested to find out whether these human based threats existence differ among banks in Malaysia. Therefore we formulated the following hypotheses:

H1. There is a significant difference between bank's branch managers' experience on the human intentional threats.

H2. There is a significant difference between bank's branch managers' experience on the human unintentional threats.

2.3 Human Based Security Control

Employees are drivers of the organization, as such human failure would adversely affect all aspects in the organization. In lieu of that, appropriate policies and procedures should be in place in order to avoid outrages, errors, loss or destruction of data, and other problems related to human failure. Therefore, our next research question is:

RQ2. To what extent, human based security controls are being reviewed in banks in Malaysia?

3.0 Research Methodology

The population of the study comprises of the conventional banks, conventional bank branches with Islamic window and Islamic banks, within Kuala Lumpur, Malaysia. There are 413 bank branches within the Kuala Lumpur district. After using a sampling technique, a total of 201 questionnaires were sent to the targeted respondents (i.e. the banks' branches managers) via mail. But, only seventy six (76) questionnaires out of 201 were returned indicating 38% response rate. We adopted cross tabulation analysis (CTA) for analysing the threats and existence of security controls in all banks branches (RQ1 and RQ2). For H1 and H2, we used seven items to measure intentional human threats and two items for unintentional threats. These items are derived from prior literature. (i.e. Abu Musa, 2006). To test these hypotheses, the Kruskal-Wallis is applied because the distribution of the data was not normal.

4.0 Results and Discussion

Our respondents consist of conventional bank with Islamic window with the highest rate of percentage, 47.4% (36), followed by conventional banks, 31.6% (24) and Islamic bank, 21.1% (16) of the total branches.

4.1 Intentional Human Threat

Our analysis depicted that a total of 15 respondents (19.7%) reported that their banks did not face this type of threats. 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 (7.9%) declared that they were most likely to be attacked by the threat. In a nut shell, bankers believed that intentional human threat least likely to occur in the banks.

The result in Table 1 reveals no significance difference among bank types in all the intentional human threat (at significant level of p=0.05) except unauthorized copy of output which is (significant at p= 0.05). Hence, hypothesis 1 (H1) was rejected because there was no significant difference in human intentional threat among the type of bank branches. This could be since all the bank branches were computerized, they were susceptible to face similar threats.

Table 1
Kruskal Wallis Test – Intentional Human Threats

Accounting Information System security Threat	Chi-Square	Df	Asymp. Sig.
Intentional entry of bad data by employees.	2.439	2	.295
Intentional destruction of data by employees.	0.301	2	.860
Unauthorized access to the data and/or system by employees.	0.622	2	.733
Employees' sharing of passwords	3.302	2	.192
Creation of fictitious/incorrect output.	2.094	2	.351
Theft of data/information	1.270	2	.530
Unauthorized copying of output.	6.596	2	**.037**

4.2 Unintentional Human Threat

The analysis revealed that majority of the respondents believed that their banks are likely to face unintentional human threats which constituted approximately one-third of the respondents. Whilst, 23.7% believed that their banks are likely to confront this type of threats. However, 32.9% of respondents have the perceptions that their banks' branches are not likely or least likely, to face such threats respectively. From the Kruskal Wallis test, it shows that there is no significant difference among different types of banks' branches about the unintentional human threat elements (at p = 0.05), as shown in Table 2. Therefore, the research hypothesis two (H2) is not supported. It is noted that there is no significant difference in human unintentional threat among the types of banks' branches.

Table 2
Kruskal Wallis Test – Unintentional Human Threats

Accounting Information System security Threat	Chi-Square	Df	Asymp. Sig.
Accidental entry of bad data by employees.	0.816	2	.665
Accidental destruction of data by employees.	1.065	2	.587

4.3 Existence of Human Based Security Control

In exploring the degree of existence of control procedures among CBS in Malaysia, the target respondents were asked to rate of such measures in their respective banks. The rating scale ranges from one to five (i.e. rarely; occasionally; frequently; often and always), with 'rarely' as the lowest and 'always' being the highest frequency rate. There are three controls asked to the respondents:

Control 1: Personnel policies include background checks to reduce the likelihood of hiring dishonest employees.

The results show that 46.1% indicated that their banks' branches always checked potential employees' background (both professional and personal) before they were employed by the bank; with a view to reduce risk of engaging corrupt staff). Moreover, 13 respondents representing 17.1% confirmed that their banks' branches frequently applied this control policy. Also, 4 respondents reported that their banks applied such policy occasionally. While only 2 respondents stated their bank branches hardly applied this policy. Hence, Malaysian CBS were aware of the important of this control policy. Since most of them frequently implement the policy as one of their control mechanisms in moderating the occurrence of accounting information fraud. The results were consistent with the findings of Abu Musa (2004).

Control 2: A segregation of duties (i.e. authorization, record keeping and custody) is good and adequate.

The findings revealed that 55.3% of the respondents indicated that their banks' branches consistently implement segregation of duties especially in terms of accounting duties such as authorization, recording etc. Also a notable percentage (31.6%) of the respondents reported that they were executing this procedure in their banks as a routine, in order to reduce the occurrence of fraud by deceitful staff. Additionally, the result disclosed that 10.5% of the respondents indicated that their banks' branches regularly segregated duties among their employees, especially on activities related to financial matters.

Control 3: There are adequate controls to restrict physical access to information system equipment.

The statistical findings of physical access controls to information system equipment indicated that almost all the respondents (88.1%) believed that their banks' branches have always and/or often adequately restricted contact to their information system equipment. Likewise, a few of the respondents (7 or 9.2%) also affirmed that they frequently implemented such control technique. However, quite low respondents (2 or 2.6%) declared that they occasionally devised physical access control procedure. As a whole, the findings displayed that the CBS in Malaysia adequately and sufficiently implemented the control procedure in their information system security.

5.0 Conclusion

Information is a valuable and confidential asset, as such an organization should preserve it from unauthorized access. In light of this, since banks are highly concerned with the security of information, adequate security controls should constantly be reviewed to protect these assets from unauthorized use, disclosure, modification or destruction, whether accidental or intentional.

References

Abu Musa, A. (2006). Investigating the security controls of CAIS in an emerging economy: An empirical study on the Egyptian banking industry. *Managerial Auditing Journal*, 19 (2), 95-108.

Abu Musa, A. (2004). The threats of computerized accounting information systems: an empirical study on Saudi organizations. *The Public Administration Journal*, 44 (3), 59-70.

Arens, A. A., Elder, R. J. and Beasley, M. S. (2006). Auditing and Assurance Services: An Integrated Approach: Eleventh Edition, Prentice-Hall, Upper Saddle River, NJ.

Beheshti, H.M. (2004). The impact of IT on SMEs in the United States. *Information Management & Computer Security*, 12 (4), 318-127.

Dhillon G. and Torkzadeh G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal,* 16, 293–314.

Gupta A. and Hammond R. (2005). Information systems security issues and decisions for small and business: An empirical examination. *Information management & computer security, 13 (2)*, 297-310.

Khan M. S. and Barua S. (2009). The status and threats of information security in the banking sector of Bangladesh: Policies required. *Bangladesh Journal of MI,* 1(2), 1-27.

KPMG (2000): Information Security Survey 2000, Executive Summary, April, KPMG, London.

Liao X., Zhang T. and Li M. (2011). Study on internal control system of the state-owned commercial bank computer systems. *IEEE*, 1-4.

Liu D., Wang X. and Camp LJ (2009). Mitigating inadvertent insider threats with incentives, IFCA/Springer-Verlang Berlin Heidelberg.

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

Mansour E., Mohammad A. A., Missi F. and Hamdan A. (2010) Examine the existence of (SysTrust) model and its impact on Jordanian commercial banks performance. *European and Mediterranean Conference on Information Systems*. Crowne Plaza Hotel, Izmir, Turkey, July, 2009.

Martin, J. C. (2005). Trust Services: A Better Way to Evaluate IT controls. *Journal of Accountancy,* 199 (3).

Ula M., Ismail Z., and Sidek Z. M. (2011). A Framework for the governance of information security in banking system. *Journal of Information Assurance & Cyber Security,* 1-12.

Walters, L. M. (2007). A draft of an information systems security and control course. *Journal of Information Systems*, 21 (1), 123-148.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, 24 (1), 43-57.