International Journal of Industrial Management (IJIM)
ISSN (Print): 2289-9286; e-ISSN: 0127-564x; Volume 4, June 2018

THE EFFECTIVENESS OF INTERNAL AUDIT FUNCTIONS IN MANAGING CYBERSECURITY IN MALAYSIA'S BANKING INSTITUTIONS

Amanuddin Shamsuddin
Accounting Department, College of Business Management and Accounting,
Universiti Tenaga Nasional, 26700 Bandar Muadzam Shah, Malaysia.
amanuddin@uniten.edu.my

Muhamad Afi Adam
Accounting Department, College of Business Management and Accounting,
Universiti Tenaga Nasional, 26700 Bandar Muadzam Shah, Malaysia.
afiadam91@yahoo.com

Saiful Ariff Adnan
Accounting Department, College of Business Management and Accounting,
Universiti Tenaga Nasional, 26700 Bandar Muadzam Shah, Malaysia.
saifulariff111@yahoo.com

Siti Nur Izzati Madzlan
Accounting Department, College of Business Management and Accounting,
Universiti Tenaga Nasional, 26700 Bandar Muadzam Shah, Malaysia.
ettydeqty@yahoo.com

Yasreen Mohd Yasin
Accounting Department, College of Business Management and Accounting,
Universiti Tenaga Nasional, 26700 Bandar Muadzam Shah, Malaysia.
ymy_94@yahoo.com

ABSTRACT

This research aimed to explore the effectiveness of internal audit in managing cybersecurity in Malaysia's Banking Institutions. This research examined three factors that would most likely affect the effectiveness of internal audit in managing cybersecurity in Malaysia's Banking Institutions. Those factors are the awareness of internal auditors about cybersecurity, organizational policy on cybersecurity and organizational risk management on cybersecurity. This study employed survey questionnaire in getting the data from the internal auditors of the sampled banking institutions. A total of 120 questionnaires were gathered from seven commercial banks. Findings from this study showed that all the three identified factors have significant relationships with the effectiveness of internal audit in managing cybersecurity in Malaysia's Banking Institutions. The findings from this study can be used by the relevant authorities and organizations in coming up with policies and procedures to manage cybersecurity better. Besides, this study would enrich the knowledge and literature on cybersecurity in Malaysia that is still lacking presently.

International Journal of Industrial Management (IJIM)
ISSN (Print): 2289-9286; e-ISSN: 0127-564x; Volume 4, June 2018

Keywords: Cybersecurity, Internal Auditors, Banking Institutions, Malaysia

INTRODUCTION

Cyber security is now firmly at the top of the international agenda as high-profile breaches raise fears that hack attacks and other security failures could endanger the global economy (INSIGHT, 2014). The consistent threat of internet attacks is a societal issue going up against all endeavors, particularly the financial associations industry. The rise in frequency and sophistication of cyber-attacks now requires an improvement in managing or fighting it. It should be one of the main issues to be discussed by the Chief Executive Officers (CEOs), Board of Directors (BODs) as well as the Board Audit Committees (BACs) in their meetings. Meanwhile, the role of internal audit today is much more than simply compliance. Internal auditor needs to stay current with this wide-ranging business issues such as cyber threats so that it can remain relevant to the organization. These business issues carry new risk, and internal audit needs to continually monitor these risks and their potential efficiency and cost benefits across organization. Internal auditor can improve its focus so that it can more efficiently add value across the organization and maximize its influence, including allocating its resources in those areas of highest impacts to the organization.

Hence, this research aspires to explore the effectiveness of internal audit in managing cybersecurity in Malaysia's Banking Institutions. In essence, the research problems for this study are summarized as follows: Firstly, the role of internal auditor has not been specified thoroughly in managing the cybersecurity in banking institutions. Secondly, there is no clear factors are stated that affect the effectiveness of internal audit in managing cybersecurity. Thirdly, the number of data security breaches is on the rise, according to a database maintained by the Open Security Foundation (Drew, 2012), and hence the functions of the internal auditor need to be reinforced.

Therefore, the main purpose of this study is to investigate the effectiveness of the internal audit in managing cybersecurity in Malaysia's Banking Institutions. Specifically, this study is conducted to achieve the following objectives:

i. To investigate the factors that affect the effectiveness of internal audit in managing cybersecurity in Malaysia's Banking Institutions.
ii. To examine the relationship between the factors and the effectiveness of internal audit in managing cybersecurity.

THEORETICAL REVIEW

Cybersecurity is a certainly fundamental danger to overall banking institutions. According to Deloitte (2016), banking institutions are the prime centres for activists, sorted out

wrongdoing, and computerized terrorists. A cyber-attack on these institutions would cause the loss of basic data and can devastatingly influence the organization's reputation, costing immense measures of time and money to repair. In addition, Romanosky (2011) pointed out that the interconnections of banking institutions leave them vulnerable to disruption, undermining national security and the quality of the worldwide banking system.

According to the report by the Pricewaterhouse and Coopers (PwC), data security breaks are growing. In 2003 there were 21 transparently reported scenes of broad scale setback, robbery, or presentation of really identifiable information. By 2011, the amount of events had extended to 1,037, and 2012 looks at risk to beat that total (PwC, 2012).

Presently, it has turned out to be progressively basic to open up any significant daily paper and discover a feature declaring the most recent data security breach. Large portions of these occurrences result in business disturbance, loss of income, extra costs and bad reputation harm. Organizations of numerous sorts and sizes are encountering an upsetting number of cybersecurity issues, challenges and fail to analyse. Information Technology (IT) divisions obviously have real obligations attending to these areas. Cyber-attacks are the reality of business today (KPMG[a], 2015) but a strong internal audit function can provide the holistic approach to cybersecurity that needed to survive (Sheridan, 2015).

In this matter, internal auditors need to be out in front, leading the business units with regards to the internal control system and also focusing on strategic business objective. Today's businesses rely on sophisticated electronic technology in every aspect of their operations and require timely information to make decisions regarding global operations. The number of data security breaches is on the rise, according to a database maintained by the Open Security Foundation (Drew, 2012). Therefore, the internal audit must operate effectively to achieve the highest results in managing cybersecurity (KPMG[b], 2015). The primary center cybersecurity function is to recognize the bank's cybersecurity risk, which is the measure of risk posed by a financial institution's activities, associations, and operational strategies. A risk is the potential for misfortune, harm, or destruction of an asset (Sheridan, 2015).

The role of internal audit is basically to improve the internal control, governance and enterprise risk management (ERM). Each organization will have the internal audit for the purpose to measure and monitoring the risk. The risk will be measured based on the organization governance, operation and information system. Likewise, the internal audit department in a banking institution must be free from the activities which it controls and should be independent from day-to-day internal control procedures. Internal audit must be unbiased and impartial, meaning that it should carry out the activity free of uncertainty and interference.

The internal audit group is in charge of giving target certification to the board and executive management on how viably the organization evaluates and deals with its cybersecurity risks. Without this guarantee, which internal audit is frequently qualified to give, the organization

runs a more serious risks of its security and protection works on getting to be lacking or even out of date Deloitte (2015).

Internal auditor additionally assume an indispensable part in working so as to secure the association intimately with official administration and utilitarian pioneers to guarantee that cybersecurity is joined into the stream of regular business and its huge number of procedure. While information security breaches is expanding, internal audit assume a basic part in giving certification around information security and protection controls and practices.

This strengthens the idea that safeguarding against cybersecurity threats is not an issue that can be tended to by any one bank. To adequately deal the diligent threats of cyber-attacks, banking institutions and bank regulators must meet up, work together, distinguish potential weaknesses, and offer industry standards and best practices (PwC, 2014).

There are however frequent and severe disciplinary actions which affect the effectiveness of internal audit in managing cybersecurity. In preliminary investigations reveals the findings about the cybersecurity represents a major focus for internal audit programs. Continuing with this current research, there is significant need for cybersecurity risk management improvement and to be very effective at managing cybersecurity risk to an acceptable risk.

RESEARCH METHOD

There are 39 bank institutions listed under licensed banking institutions which comprises of commercial banks, Islamic banks, international Islamic banks, investment banks and other financial institutions. The sampling frame was obtained from commercial banks because of the large number listings of bank institution and these types of banks have high growth prospects. There are 27 commercial banks registered under Bank Negara Malaysia's list of licensed banking institution in Malaysia and hence the sample size for this study consists of these 27 banking institutions. The purpose of the data collection is to answer the three research objectives above.

Besides content analysis, data for this study was collected via survey questionnaires and semi-structured interviews with internal auditors who are working in banking institutions at Kuala Lumpur, based on the convenient sampling. The questionnaire was adapted from Steinbart (2012), Ernst & Young (2014) and Alkafaji et al. (2013). Besides, the questionnaire was also based on the internal control questionnaires (ICQs) that are normally used by the internal auditors in carrying out their functions.

The target respondents were the internal auditors for the commercial banks. The respondents were required to answer the questionnaires using four point interval scales. Four point scales ranges from range 1 until 4 which are represented by strongly disagree (1), disagree (2), agree (3) and strongly agree (4). This scale were used since it is supported by Worcester and Burns (1975) which mention that four point scale without a mid-point appears to drive more

International Journal of Industrial Management (IJIM)
ISSN (Print): 2289-9286; e-ISSN: 0127-564x; Volume 4, June 2018

respondents towards the positive end of scale. The questionnaire was distributed to 150 respondents; however, only 120 respondents took place in this survey (80% response rate).

Factor analysis was used to analyse the data in order to identify the important factors that contribute to the effectiveness of internal audit in managing cybersecurity in banking institutions in Malaysia. Subsequently, descriptive statistics and multiple regressions were conducted to examine the effectiveness of the internal audit functions as well as investigate the correlation of the factors and the effectiveness of internal audit roles in managing cybersecurity. The results of the analysis were summarised and a model was developed based on the factors identified that would enhance the roles of internal audit in managing cybersecurity.

RESULTS AND DISCUSSION

For the first objective, the effectiveness of the internal audit functions was measured using five questions as shown in Table 1. Based on the results displayed in Table 1, the overall mean score of 16.47 indicates that majority of respondents agreed that internal auditors had been effective in carrying out their functions in managing the cybersecurity.

In determining the factors that affect the effectiveness of internal audit in managing cybersecurity (objective 2), the factor analysis was performed. It was found that the factors such as the awareness, organizational policy and risk management on cybersecurity emerged as the significant factors in ensuring the effectiveness of the internal audit in managing cybersecurity in Banking Institutions. Descriptive statistics also revealed that the means for the respective factors are high and approaching the maximum scores (see Table 2).

Table 1: Effectiveness of the Internal Audit Functions

No.	Statements	Minimum	Maximum	Mean	Std. Deviation
1.	Assessment tool to identify recommended baseline controls all financial institutions should have in place.	2	4	3.47	.549
2.	There are ways to address and track deficient internal controls and follow up.	2	4	3.38	.624
3.	There are conceptual tool for identification of gaps and vulnerabilities within your IT program.	2	4	3.05	.563
4.	Creativity and efficiency is created when using innovation of technology.	2	4	3.23	.493

International Journal of Industrial Management (IJIM)
ISSN (Print): 2289-9286; e-ISSN: 0127-564x; Volume 4, June 2018

5.	Employee security, access management, financial-related controls, event logging, and vendor management are in a good condition.	2	4	3.34	.558
	Total			**16.47**	**2.787**

Table 2: Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Awareness	120	16.00	32.00	25.9417	3.16572
Policy	120	20.00	32.00	27.2417	2.80155
Risk Management	120	18.00	32.00	26.7333	3.08897
Effectiveness	120	13.00	20.00	16.4667	2.07803
Valid N (listwise)	120				

The third objective of this study was to examine the relationship between the factors and the effectiveness of internal audit in managing cybersecurity. This study used Spearman correlations to measure the relationship between independent variables (awareness, policy, risk management) and dependent variable (internal audit effectiveness) in managing cyber security in Malaysia's banking institutions. Spearman correlation was used because the data was not normally distributed. Table 3 shows the correlation results.

Table 3: Results of the Correlation Analyses

		AWARENESS	POLICY	RISK MANAGEMENT	EFFECTIVE-NESS
AWARENESS	Spearman Correlation	1	.483**	.570**	.285**
	Sig. (2-tailed)		.000	.000	.002
	N	120	120	120	120
POLICY	Spearman Correlation	.483**	1	.576**	.342**
	Sig. (2-tailed)	.000		.000	.000
	N	120	120	120	120
RISK MANAGEMENT	Spearman Correlation	.570**	.576**	1	.479**

International Journal of Industrial Management (IJIM)
ISSN (Print): 2289-9286; e-ISSN: 0127-564x; Volume 4, June 2018

	Sig. (2-tailed)	.000	.000		.000
	N	120	120	120	120
EFFECTIVENESS	Spearman Correlation	.285**	.342**	.479**	1
	Sig. (2-tailed)	.002	.000	.000	
	N	120	120	120	120

**. Correlation is significant at the 0.01 level (2-tailed).

Based on Table 3 above, the p-value of awareness of cyber security and the effectiveness of the internal audit functions for Malaysia's banking institutions is 0.002 which is less than 0.05. This shows that there was significant positive correlation between awareness and effectiveness of the internal audit functions in managing cyber security. The positive correlation indicated that when the level of internal auditors' awareness increases, the effectiveness of the internal audit functions in managing cyber security also increases. Table 3 also shows that the correlation coefficient value is 0.285 which indicated a small relationship between internal auditors' awareness and effectiveness of the internal audit functions in managing cyber security (Cohen, 1988). In addition, MOSTI (2011) stated that Malaysian government security agency; Cybersecurity Malaysia said that Malaysians need to become even more security-aware. The level of awareness among Malaysian internet users on safety issues in cyberspace need to be strengthened (NIST, 2014).

As for the second factor, organisationa policy, the p-value of policy on cyber security and the effectiveness of the internal audit functions for Malaysia's banking institutions is 0.000 which is less than 0.05. This indicates that there was significant positive correlation between organizational policy on cyber security and the effectiveness of internal audit functions. The positive correlation shows that as the level of organizational policy increases, the effectiveness of internal audit functions increases. Table 3 also shows that the correlation coefficient value is 0.342 which presents medium relationship between organizational policy on cyber security and the effectiveness of internal audit functions. In addition, Ernst & Young (2014) stated that internal auditor could assist to recognize gaps in the policies and procedures that are carried out in the organization which related to information security. Other than that, Symantec (2015) suggested that cybersecurity policies could also be evaluated by internal audit.

Results shown in Table 3 also indicate that there is a positive significant relationship between the organizational risk management and the effectiveness of internal audit functions as the p-value is 0.000 which is less than 0.05. The correlation coefficient value is 0.479 which presents medium relationship between organizational risk management on cyber security and the effectiveness of internal audit functions. As stated by Basel Committee in June, 2012, a bank's risk management operates support and considers its adherence to administrative arrangements and protected banking activities (Robert (2012). Moreover, William and Zheng

(2015) also stated that internal audit should take the following features of risk management functions which comprise of market, credit, liquidity, interest rate, operational and legal risk.

CONCLUSION

The main purpose of this research is to explore the effectiveness of internal audit in managing cybersecurity in Malaysia's Banking Institutions. The outcomes of the study indicate that internal auditors were effective in managing cybersecurity based on the survey conducted. Meanwhile, factors such as awareness, organizational policy and risk management on cybersecurity emerged as the important factors in ensuring the effectiveness of the internal audit in managing cybersecurity in Banking Institutions. In addition, based on the correlation analyses conducted, this study found out that awareness, organizational policy, risk management and the effectiveness of internal audit functions shows positive significant correlations. These results could be used as a platform for creating a new and improve auditing standards in order to enhance the effectiveness of internal audit involving cybersecurity.

As for the contributions, findings form this study are hoped to contribute to the literature in gaining the information and understanding about the effectiveness of internal audit in managing cybersecurity in Malaysia's Banking Institutions. This contribution would enhance the roles and functions of internal audit in managing cyber security in other organizations as well. Moreover, this study would be helpful to the practitioners in training and informing them in areas of the importance on how to make the role of internal audit become more efficient in raising their skills and understand the latest threats. Besides, it also helps them in providing assurance for many facets that make up data security. In addition, this study also helps the policy implications in obtaining a guideline that might assist them for responding to cyber-attack and reducing the threat of cyber terror.

REFERENCES

Alkafaji, Y.A., Majdalawieh, M. and Zaghloul, I. (2013), How Technology is Shaping Internal Auditing, UAE Internal Auditors Association.

Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.), Hillsdale, NJ: *Lawrence Earlbaum Associates*.

Deloitte (2016), Cybersecurity: A good defense isn't enough; 2016 Global Impact Report.

Deloitte. (2015). Cybersecurity: The changing function of audit committee and internal audit.

Cyber security level in Malaysia better than those in developed countries. (2009). Retrieved October 2011, from

http://www.cybersecurity.my/en/knowledge_bank/news/2009/main/detail/1725/index.html

Drew, J. (2012). Managing Cybersecurity Risks. *Journal of Accountancy*, 214(2), 44-48

Ernst & Young (2014), Get ahead of cybercrime EY's Global Information Security Survey 2014, *Insights on governance, risk and compliance*, October.

INSIGHTS (2014) Cyber Security and Related Issues: Comprehensive Coverage, November 26, 2014 Retrieved October 2011, from www.insightsonindia.com/.../cyber-security-related-issues-comprehensive-coverage

KPMG[a] (2015). Cyber Security Dashboard: Monitor, Analyse and Take Control of Cyber Security.

KPMG[b] (2015). Top 10 key risks in 2015. KPMG Internal Audit.

MOSTI (2011), Cloud Security Alliance, Cyber Security Forum Initiative and CyberSecurity Malaysia, *Conference on Cybersecuriy Asia*, Singapore

NIST (2014), National Institute of Standars and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0

PwC. (2014). Threat smart: Building a cyber resilient financial institution, *Viewpoint*, Vol. 49.

PwC. (2012). Fortifying your defenses: The role of internal audit in assuring data security and privacy, *Viewpoint*, Vol. 39

Robert, O. (2012): Cyber security in the financial sector Basel Committee Report, June, 2012

Romanosky, R. T. (2011). Do data breach disclosure laws reduce identity theft?, *Journal of Policy Analysis and Management*. Vol. 30, No. 2, pp. 256–286.

Sheridan, T. (2015). Internal Audit Taking a More Holistic Approach to Cybersecurity.

Steinbart, R. L. (2012). The relationship between internal audit and information security: An exploratory investigation. *Journal of Policy Analysis and Management*. Vol. 30, No. 2, pp. 114–128.

Symantec (2015). Strategies that Empower your Business, Drive Innovation and Build Customer Trust. *Cyber Security for Financial Services*.

William A. C. and Zheng, D. E. (2015), The Evolution of Cybersecurity Requirements for the U.S. Financial Industry, *Centre for Strategic and Internationa Studies (CSIS*), July, Washington.