An Analysis of Computerized Accounting System Security Threats in Malaysian Public Listed Companies

[1]Mahlindayu Tarmidi @ Tokhid*, [1]Azwan Abdul Rashid
and [1]Wan Mohamad Taufik Wan Abdullah
[1]Department of Accounting, College of Business Management and Accounting,
Universiti Tenaga Nasional, Sultan Haji Ahmad Shah Campus,
26700 Bandar Muadzam Shah, Pahang, Malaysia.
*Corresponding e-mail: mahlindayu@uniten.edu.my

Abstract

Numbers of incidents pertaining data errors, system breach, violation of internal control and manipulation of financial information had raised the organization attention and concern. Organizations are consequently more aware of the security and integrity issues in regards of the computerized accounting system and the need to take appropriate action. This research is to investigate the security threats issues in computerized accounting system in Malaysian public listed companies. Through questionnaires to 500 companies, the study is expected to determine the companies' most important perceived security threats, and variations among the industries and organization size. The empirical evidence may enable organizations to evaluate their computerized accounting system security, and begin to properly pursue effective strategies to improve quality and lower risk.

Keywords: *Computerized accounting system, Information security threats*

1. INTRODUCTION

The main product of information system in organisations is financial information. Accountants need to be familiar with the risk associated with their computer system in order to protect this information. Technology had exposed the organisation information security in risk. The risk is no longer lies on the information system, but also includes loss of trust, legal liabilities and severe financial damages (Mc Adams, 2004). Numbers of reports can be found in regards of financial reporting errors, thefts, violation of internal control and sabotage (Abu Musa, 2006). The AICPA technology division had laid down that Accounting Information System security is a primary technological concern (Davis, 1997). Hence, companies need to pay more focus on the financial security issues in addition to the whole information system security to ensure the reliability of their information.

The theoretical significance of this study arises from insights into the existing body of theory and further, from theorizing about the perceived information system security threats in Malaysia public listed companies. At the same time, this study also serves as a practical reference for the development of the awareness on the subject matter. Only with a clear understanding of actual threats in computerized accounting information system, organizations could define their implementation of security tasks more successfully. Therefore, this paper is to investigate the security threats issues in computerized accounting system in Malaysian public listed companies. Using an adopted security checklist developed by Abu Musa (2007), the research thus attempts to answer the following research questions:

RQ1: What are the perceived threats of computerized accounting information systems (CAIS) in Malaysia Public Listed Companies?

RQ2: Are there a significant different among different industries and companies size in regards of perceived security threats in their CAIS?

The rest of the paper is organized as follows. The next section offers a review of literature on ERP followed by the discussion on the research methodology and the research findings. The final section concludes with the research summary.

2. LITERATURE REVIEW

Most of previous research had paid more attention on the information security as a whole. They are more concern in investigating the threats on computerized system, the security threats to the real world and estimation of losses as results of the event. There is not much study done focusing on computerized accounting information system as it is considered as a new topic (Abu Musa, 2007). Loch et al. (1992) had contributed a meaningful contribution on their study of executives' perception towards their management information system. The result reveals twelve security threats and has ranked these four threats as the highest. Those are Natural disaster, accidental employees' actions, inadequate media control and unauthorised access to their CAIS. Davis, 1997 in his study had found, among the source of security threat is natural disaster. External factors such as virus attacks, worms, system hacking and spyware are among the highest rank listed by Gartner Group (Brynes, 2005).

Focusing in the computerised accounting environment, number of studies prevail the internal forces which contributed to information security threats. Employees may play a vital role if they are not fully train and enforced the awareness about system security. Among the incident happened as a result of employees weakness are accidental entry of bad data, accidental destruction of data, intentional data destruction, misinterpreted of data, misused of data and improper use of data. (Davis, 1997, Ryan and Bordoloi, 1997, Siponen, 2000 and Dhillons ,1999). Abu Musa (2007) supported in his study which proof that the most threats to organisation information system are from insider not outsider. A study conducted by Wright and Wright (2002) discussed that among the reason for such employees contribution in such threats is lack of training. Dhillon, 1995, argued that an organisation may reduce the insider attack if they applied a pragmatic approach which emphasise on technical, formal and informal interventions in their computerised system.

Internal auditors also may play a vital role in contributing the security of information system (Coffin and Patilis, 2001). But the problem is to get them involve in the security audit is a challenge. Internal auditors are more focus on internal IT risk and control such as application processing, IT assets safe guarding and data integrity (Hermanson, 2000). In some other cases, they are less concern in IS auditing. They responsibility is perceived to be done by the information system auditors (Hunton et al., 2004). In the context of Malaysia, a study was done by Dzazali, Sulaiman and Zoliat (2009). One of the discussions on security incidents in Malaysia Public Service Organisation highlighted that 25% of the incidents were originated by insiders, 11% was the combination of internal and external forces. This actually in line with the survey result by Ernst and Young (2004) and NISER (2004), which indicate that most threat to information security are from inside the organisation.

3. METHODOLOGY

The study was carried out on the Malaysian public listed companies both on the first and second boards of Kuala Lumpur Stock Exchange. The non-probability convenience sampling design was chosen as is most often used method during the exploratory phase of a research project (Sekaran, 2003). Questionnaires were posted out to 500 companies and 266 returned and 252 were used for this analysis. The questionnaire was adapted from one used by Abu Musa (2006), who explored the perceived threats of computerized accounting information system in Saudi Arabia. It was divided into two parts, which is the first part inquire on the companies' information and the second part, the respondents are required to rate, based on a six-point Likert type scale (1= not sure/never;, 2= less than once a year; 3= once a year to monthly; 4= once a month to weekly; 5=once a week to daily; 6=daily or more frequently), the threats in accounting information system.

Manufacturing companies constitute the majority of the sample (32.9%), and most of the companies (66.7%) have one to fifty accounting professional. 34.5% of the respondent held one to five IS specialist in the organization. Reflecting the major respondents are from manufacturing sector, 35.7% from the total respondents have 1000 employees. Out of 252 respondents, 146 companies (57.9%) are operating in a strongly computerized accounting environment. It was observed that more than half of the companies (53.2%) had suffered loss form security breach by both internal and external factors. 32.9 % are suffering from internal threats and 13.9% are from external sources of threats. The findings thus in line with (KPMG, 2000, Green, 2003 and Swann, 2004) Table 1 further explained in details the companies' information.

4. RESULTS AND FINDINGS

The result is based on the 19 threats listed in the questionnaires and the findings are discussed by answering the research questions provided earlier. In order to rank the results, the study look at the average score, Mean, of the responds. Based on the results gathered, the overall view portrays that the most respondents perceived that the 19 listed threats occurs in their organisation in less than once a year to monthly basis. Very little of them view it as a severe threats which might happened on weekly to daily basis.

The highest mean is for accidental entry of bad data by employees. With mean of 2.2, 37.70% of the respondent believed it occurs on once a year to monthly basis. Though 25.4% perceived the occurrence is less that once a year, but 24.21% indicated it occurs once a month to monthly basis. Respondents perceived introduction (entry) of computer viruses to the system as the second CAIS threats. It was also considered as the most frequent threats to occur. Out of 242 companies, 79 perceived it to happen on once a year and monthly basis while 13 of the respondent believed it occurred on daily basis. 2 respondents had never experienced such threats and 78 had rarely experience it. The study also reveals that an internal factor is perceived to be a contributor of the threats. Employees plays the vital role in all organisations and the study reveals the mean of 1.89, 39.68% of the respondents perceived accidental destruction of data by employees as the third threats in CAIS though it is perceived to occur in less that once a year. But 89 respondents agree the occurrence of such threats is once a year to monthly. This goes hand in hand with another listed a threat which is unauthorized access to the data and/or system by employees.

Employees sharing password are also seemed to be another threat (mean = 1.83). Only 2 companies (0.79%) had never experienced this, but 44 companies declared this threat is perceived to happen on monthly to weekly basis. 7.54% of respondents indicated, such threat happen in their organisation on weekly to daily basis. Most of the respondents, 74.21%, perceived the threat to happen on once a year to monthly basis. Another internal force that rise threats to CAIS is Suppression or destruction and creation of fictions or incorrect output. Though 46.03% of respondents claim it only happened less than once a year, but more than 47% agreed it occurs on monthly to daily basis.

The least threats perceived is natural disaster (mean = 1.46). 65.08% (164 respondents) indicated they only experience such threats in less than once a year. Hence, the threats it self is beyond human controls, it may be one reason why the threats is considered as the least. Human disaster such as fire, loss power is perceived as another least threats to CAIS. 6 respondents perceived it to happen on daily basis, but 83.73% of respondents agreed it might occur on less than once a year to monthly basis. Only 33 companies perceive the occurrence on weekly to daily and 2 companies had never experience it. The detail of all 19

CAIS threats is ranked in Table 2 together with the frequencies of occurrence perceived by the respondents.

The results also tend to provide evidence on any significant different among different industries and companies size in regards of perceived security threats in their CAIS. The results of Spearman Correlation at significant level p = 0.05, portrays that there is no significant different between different industries, number of employees and total assets regarding the occurrence of the threats, except for Unauthorized copying of output, Intentional destruction of data by employees and Unauthorized access to the data and / or system by outsiders (hackers). The result is listed in Table 3.

Table 1: Companies information

Type		Frequency	Percent
Categories	Manufacturing	83	32.9
	Construction	46	18.3
	Trading	37	14.7
	Services	3	1.2
	Technology	10	4.0
	Finance/banking	19	7.5
	Hotels	16	6.3
	Properties	13	5.2
	Plantation	21	8.3
	Closed/fund	4	1.6
No. of Accounting professional	1-50	168	66.7
	51-100	49	19.4
	101-150	18	7.1
	151-200	7	2.8
	over 200	10	4.0
No. of IS specialist	1-5	87	34.5
	6-10	58	23.0
	11-15	44	17.5
	16-20	34	13.5
	over 20	29	11.5
No. of employees	<250	37	14.7
	250 - 500	65	25.8
	501 - 1000	60	23.8
	>1000	90	35.7
Type of accounting system	A combination between manual and computer processed	106	42.1
	Strongly computerized	146	57.9
Loss suffered due to security breach by	Employees (internal sources)	83	32.9
	Outsider (external sources)	35	13.9
	Both	134	53.2

Table 2: CAIS security threats

Computerized Accounting Information Systems (CAIS) security threats		Mean	S.D.	Frequencies of CAIS Security Threats												
				Not sure/ Never		Less than once a year		Once a year to monthly		Once a month to weekly		Once a week to daily		Daily or more frequently		Total
1	Accidental entry of bad data by employees	2.2	1.061	1	0.40%	64	25.40%	95	37.70%	61	24.21%	22	8.73%	9	3.57%	252
2	Introductions (entry) of computer viruses to the system	2.17	1.125	2	0.79%	78	30.95%	79	31.35%	63	25.00%	17	6.75%	13	5.16%	252
3	Accidental destruction of data by employees	1.89	0.983	1	0.40%	100	39.68%	89	35.32%	43	17.06%	14	5.56%	5	1.98%	252
4	Unauthorized access to the data and / or system by employees	1.86	0.993	1	0.40%	106	42.06%	90	35.71%	33	13.10%	17	6.75%	5	1.98%	252
5	Employee's sharing of passwords	1.83	1.055	2	0.79%	121	48.02%	66	26.19%	44	17.46%	10	3.97%	9	3.57%	252
6	Suppression or destruction of output	1.83	0.998	2	0.79%	116	46.03%	73	28.97%	43	17.06%	13	5.16%	5	1.98%	252
7	Creation of fictions/ incorrect output	1.79	0.978	0	0.00%	116	46.03%	84	33.33%	36	14.29%	9	3.57%	7	2.78%	252
8	Prints and distributed information are directed to people who are not entitled to receive it	1.77	1.043	4	1.59%	124	49.21%	74	29.37%	32	12.70%	7	2.78%	11	4.37%	252
9	Unauthorized document visibility by displaying on monitor or printed on paper	1.76	0.929	3	1.19%	114	45.24%	88	34.92%	35	13.89%	6	2.38%	6	2.38%	252
10	Printing and distribution of information by unauthorized persons	1.75	1.006	1	0.40%	126	50.00%	76	30.16%	31	12.30%	10	3.97%	8	3.17%	252
11	Interception of data transmissions from remote locations	1.71	1.011	3	1.19%	129	51.19%	81	32.14%	20	7.94%	9	3.57%	10	3.97%	252
12	Unauthorized copying of output	1.68	0.903	4	1.59%	129	51.19%	74	29.37%	33	13.10%	9	3.57%	3	1.19%	252
13	Sensitive documents are handed to non-security cleared personnel for shredding	1.67	0.948	2	0.79%	139	55.16%	65	25.79%	29	11.51%	14	5.56%	3	1.19%	252
14	Intentional destruction of data by employees	1.66	0.954	2	0.79%	143	56.75%	60	23.81%	30	11.90%	14	5.56%	3	1.19%	252
15	Intentional entry of bad data by employees	1.66	0.908	1	0.40%	136	53.97%	71	28.17%	31	12.30%	10	3.97%	3	1.19%	252
16	Unauthorized access to the data and / or system by outsiders (hackers)	1.63	0.91	2	0.79%	141	55.95%	71	28.17%	21	8.33%	15	5.95%	2	0.79%	252
17	Theft of data / information	1.62	0.924	3	1.19%	145	57.54%	61	24.21%	30	11.90%	9	3.57%	4	1.59%	252
18	human made disaster such as fire, loss power	1.6	0.934	2	0.79%	150	59.52%	61	24.21%	26	10.32%	7	2.78%	6	2.38%	252
19	Natural disaster such as fire, flooding, loss of power	1.46	0.8	4	1.59%	164	65.08%	60	23.81%	15	5.95%	6	2.38%	3	1.19%	252

Table 3: Spearman correlation result

Computerized Accounting Information Systems (CAIS) security threats		Spearman Correlation					
		No. of employees		Total Assets (RM)		Organization's classification	
		Correlation Coefficient	Sig	Correlation Coefficient	Sig	Correlation Coefficient	Sig
1	Accidental entry of bad data by employees	0.020	0.752	0.040	0.549	0.005	0.931
2	introductions (entry) of computer viruses to the system	0.032	0.608	0.048	0.472	-0.008	0.895
3	Accidental destruction of data by employees	-0.051	0.412	0.023	0.730	-0.075	0.234
4	Unauthorized access to the data and / or system by employees	0.058	0.353	-0.019	0.775	-0.039	0.531
5	Employee's sharing of passwords	0.050	0.423	-0.108	0.105	-0.041	0.510
6	suppression or destruction of output	-0.022	0.721	-0.066	0.327	0.003	0.963
7	Creation of fictions/ incorrect output	0.000	0.996	-0.051	0.446	0.035	0.573
8	Prints and distributed information are directed to people who are not entitled to receive it	0.025	0.695	-0.016	0.807	-0.040	0.523
9	Unauthorized document visibility by displaying on monitor or printed on paper	0.018	0.774	-0.084	0.212	0.018	0.775
10	Printing and distribution of information by unauthorized persons	0.109	0.082	-0.067	0.317	-0.031	0.620
11	Interception of data transmissions from remote locations	-0.056	0.377	-0.082	0.220	0.037	0.556
12	Unauthorized copying of output	0.075	0.234	-.133*	0.049	-0.078	0.215
13	Sensitive documents are handed to non-security cleared personnel for shredding	-0.033	0.604	-0.129	0.054	-0.042	0.499
14	Intentional entry of bad data by employees	-0.079	0.208	-0.034	0.611	0.003	0.960
15	Intentional destruction of data by employees	-.145*	0.021	-0.125	0.061	0.004	0.951
16	Unauthorized access to the data and / or system by outsiders (hackers)	0.087	0.164	-.156*	0.020	-0.044	0.483
17	Theft of data / information	0.054	0.390	-0.065	0.336	0.010	0.869
18	human made disaster such as fire, loss power	0.091	0.147	0.023	0.735	0.055	0.377
19	Natural disaster such as fire, flooding, loss of power	0.070	0.266	0.022	0.742	-0.053	0.403

5. CONCLUSION AND FUTURE RESEARCH

The article delivers an exploratory overview of the perceived degree of computerized accounting system security threats in Malaysia particularly among the listed companies across the industry. As there is limited prior academic research on CAIS threats in Malaysia, this research may provide an insight of perceive information system threats especially in computerized accounting environment. This may benefit the regulators and companies on the threats issues and may trigger the awareness to improve their security systems. The study had adopted 19 computerised accounting threats listed by Abu Musa (2006) in his previous study. The findings reveal that most of CAIS security threats are originated by the internal source which is the employees. Accidental entry of bad data by employees was considered as the most frequent threats to happen. Apart of that accidental destruction of data by employees and unauthorised access of data and system by employees also perceived as the most common threats among the respondents.

This is in line with the study done Wright and Wright (2002) and they had suggested the reason could be the lack of skills and training among the employees. The findings also support the previous study done Ernst& Young (2004), Niser (2004) and Abu Musa (2007). This study also found viruses is the most threats from external forces. This is supporting the result of Brynes (2005). This does reflect the losses faced by 53.2% of the respondent who suffering losses caused by both internal and external source. Opposing the result gathered by Davis (1997), natural and human made disaster was found to be the least threat perceived among the listed companies. Other least threats perceived are also theft of data and intentional entry of bad data of employees. The study also prevails the perceived degree of occurrence of the listed threat in their organisation. Generally, respondents rated the 19 threats only occur in less than a year to year to monthly basis. This could propose the sign of proper internal control and security implemented in their organisations. However, a further research could be undertaken to further discuss the issue. Future research may look at the impact of the CAIS threats in term of company financial reporting and performance and other related areas.

References

Abu-Musa, A. A. (2006). Perceived security threats of computerized accounting information systems in the Egyptian banking industry. *Journal of Information Systems,* 21(4), 387-407.

Abu-Musa, A. A. (2007). Evaluating the security controls of CAIS in developing countries: An empirical investigation. *Information Management & Computer Security,* 15(2), 128-140.

Brynes, C. (2005). *The Gartner group: Information security trends 2005–2007.* Retrieved July, 2006, from http://www.gartner.com

COBIT (2002). *Control objectives for information and related technology, by the information systems, audit, and control foundation.* Illinois, USA: ISACA, 1997. Retrieved January 15, 2010, from http://www.isaca.org/cobit.htm

Coffin, R. G., & Patilis, C. (2001). The internal auditor's role in privacy. *Internal Auditing*, 16(2), 22-28.

Davis, C. E. (1997). An assessment of accounting information security. *The CPA Journal*, 67(3), 28-34.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security*, 7(4), 171-175.

Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organisations. *Government Information Quarterly*, 26, 584-593.

Ernst & Young (2004). *Ernst & Young global information security survey* 2004. Retrieved March 28, 2010, from http://www.ey.com

Green, M. (2003). Securing the system. *Best's Review*, 103(10), 80-84.

Hermanson, D. R., Hill, M. C., & Ivancevich, D. M. (2000). Information technology-related activities of internal auditors. *Journal of Information Systems, Supplement,* 14(1), 39-53.

Hunton, J., Wright, A. & Wright, S. (2004). Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems? *Journal of Information Systems,* 18(2), 7-28.

KPMG (2000). Information security survey 2000, Executive summary, KPMG, London. Retrieved March 28, 2010, from http://www.kpmg.bb/uploads/bb/best _of_irm_insights_part_2.pdf

Loch, K. D., Houston, H. C., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly,* June, 173-186.

McAdams, A. C. (2004). Security and risk management: A fundamental business issue. *Information Management Journal,* 38(4), 36−44.

NISER (2004). NISER ICT Security Survey for Malaysia 2004. Retrieved March 28, 2010, from http://www.niser.org

Ryan, S. D., & Bordoloi, B. (1997). Evaluating security threats in mainframe and client / server environments. *Information & Management,* 32(3), 137-142.

Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(8), 31-44.

Solms, B., & Solms, R. (2004). The 10 deadly sins of information security. *Computers and Security*, 23(5), 371−376.

Swann, J. (2004). Always on the case: Engaging your staff in bank security. *Community Banker,* 13(3), 44-47.

Wright, S., & Wright, A. (2002). Information system assurance for enterprise resource planning systems: Implementation and unique risk considerations. *Journal of Information Systems,* Supplement, 16, 99-113.