International Journal of Finance and Accounting 2013, 2(2): 109-113
DOI: 10.5923/j.ijfa.20130202.10

Computerized Accounting System Threats in Malaysian Public Services

Mahlindayu binti Tarmidi[1,*], Azwwan Abdul Rashid[1], Mohmad Sakarnor bin Deris[1], Rusli Abdul Roni[2]

1Department of Accounting. College of Business Management and Accounting, Universiti Tenaga Nasional, Bandar Muadzam Shah, 26700, Pahang
[2]Deprtment of Business and Accounting, College of Foundation and General Studies, Universiti Tenaga Nasional, Bandar Muadzam Shah, 26700, Pahang

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 services. Through questionnaires to 500 CAIS user in the Jabatan Akauntan Negara Malaysia (Accountant General Department), the study findings show the users perception of the current state of threats faced by the system. Though most of the listed threats are perceived to be rarely happen, but there are group of people indicates those incidents still taken place. Hence, this empirical evidence may enable the public services department to evaluate their computerized accounting system security, and begin to properly pursue effective strategies to improve quality and lower the risk of incidents.

Keywords Computerised Accounting System, System Threats, Jabatan Akauntan Negara

1. Introduction

The revolution of accounting systems used in Malaysian Public sector begins in early 1969, namely Program Performance Budgeting System (PPBS) for budgeting purposes. As result of difficulties in implementation, in early 19810's, a new system was introduced (MBS), with the main objective to increase the efficiency in the financial management of government specifically, to increase accountability among controlling officers and program and activities managers. In 1992, the government introduced the Macro Accounting System (MAS), which was designed to facilitate the collection, processing and preparation of the cost information, prepare information on cost efficiently and in a more flexible manner, produce reliable cost information and contribute to the optimization of the use of resources[1]. In 2006, Government Financial Management and Accounting System (GFMAS) was introduced to the Accounting General Department (AGD) of Malaysia. GFMAS helps to smoothen the financial planning, budget control and Government accounts. It combines all the accounting functions such as payment, receipts, managing salaries, Government loans, Loans and Advances to public servants. The GFMAS can record a complete budget planning, flexible to cash and accrued account, and increase the security[2].

The development showed the vital role played by Computerized accounting system (CAS) in providing most appropriate and a clear picture of accounting information's in a systematic manner. The presence of growing security threats has result in lack of confidentiality, integrity and availability of the information which affects the business activities of many organizations. Recently, CAS involves use of present technological advances. Besides make a revolution in traditional paper methods of accounting. But on the other hand, the rapid changes in technology had created significant risks in ensuring the security and integrity of CAS[3].

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. ([4],[5],[6] and[7].[8] supported in his study which proof that the most threats to organisation information system are from insider not outsider.

In the context of Malaysia, a study was done by[9]. 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

* Corresponding author:
mahlindayu@uniten.edu.my (Mahlindayu binti Tarmidi)
Published online at http://journal.sapub.org/ijfa
Copyright © 2013 Scientific & Academic Publishing. All Rights Reserved

internal and external forces. This actually in line with the survey result by[10] and[11], which indicate that most threat to information security are from inside the organisation

As reported by[12], the increase in the number of reported cyber incidents imply that the issue of security in computerised accounting system (CAS) is noteworthy. The effect of such incidents could leave the investor wary and lacking faith in the integrity of published financial reports, and to a certain extent, leading to legal liabilities and severe financial damages[13]. According to[4], the AICPA technology division recognised the importance of CAS security to help ensure the integrity of the information in the companies' financial reports in an attempt to restore investor confidence. While these companies' faces daunting challenges amid rapid technological changes, there is a growing need to better understand the security threats of CAS. Furthermore, the CAS represents the largest and vital component of management information system (MIS) environment as it provides financial information to the management[14].

This present study is timely in providing the much needed empirical evidence with a view of contributing to better understanding of security threats issues particularly in the Malaysia Public Services CAS environment. Only with a clear understanding of actual threats in CAS, the Malaysia government could define their implementation of security tasks more successfully, which in turn could enhance the integrity of its information. At the same time, this study also serves as a practical reference for the development of the awareness on the subject matter. Therefore, the purpose of this study is to investigate the perception of users on CAS threats faced by the user of GFMAS, in the Accountant General Office in Putrajaya, Malaysia.

2. Research Methodology

The population of this study was drawn from the user of GFMAS in the Accountant General Department of malaysia located in Putrajaya, Malaysia. The whole user were invited to participate in the surver and out of 500 questionnaires mailed to respondents, 331 were returned and only 323 were used for further analysis. The questionnaire was adapted from the one used by[15] who explored the perceived threats of CAIS in Saudi Arabia. It was divided into two parts, which is the first part inquire on the respondent personal information and the second part, the respondents are required to rate, based on a five-point Likert scale (1= strongly disagree;2= disagree; 3= neutral; 4= agree; 5=strongly agree), the threats in their accounting information system.

The female respondent had dominated the group (77%) with most of the respondent were at age 21-30 years old. The respondent is grouped between IT and Non-IT department as the study would try to investigate any correlation between different departments towards CAS threats. But, the users were mostly from Non-IT department which this may contribute to biasness in the result later. There were three groups of job position stated in the survey question, but only two grades were marked. Non of the respondent were JUSA, and 75% were between grade 14-40. This may related to the highest qualification held by them which is in diploma level (42%). Finally, most of the respondent only had served the section for less than 5 years (41%). Table 1 will further display the detail about the respondent background.

3. Result and Discussion

Before further analysis is done, it is crucial to test the reliability and consistency of the instrument used. Through reliability test, the Cronbach alpha was at 0.95 and all 19 items of the listed incidents were kept. The threats of accounting system may occur during data input, data processing, database and data output[16]. Hence, the 19 threats adopted were reclassified based on the four areas with human made and natural disaster in its own category, the findings are discussed in the following section. The detail findings on perception of user towards the security threats is display in detail in Table 2.

3.1. Data input

Two threats were categorize in the group and more almost 50% of the respondent agreed that accident bad data entry is considered as threats but intentional act for the incidents is perceived as not a threats. What is alarming there is still more than 20% did not really sure the perception of those incidents. This may trigger for more awareness training on the secueirt threats of data input among the system user.

Table 1. respondent personal information

		Frequency	Percent
Gender	Male	73	22.6
	Female	250	77.4
	Total	323	100.0
Age	<20 years	1	.3
	21 - 30 years	167	51.7
	31 - 40 years	106	32.8
	41 - 50 years	25	7.7
	> 50 years	24	7.4
	Total	323	100.0
Department	IT department	46	14.2
	Non-IT department	277	85.8
	Total	323	100.0
Job Position	GRED41- 54	78	24.1
	GRED 17- 40	245	75.9
	Total	323	100.0
Educational Background	Foundation/Certificate	73	22.6
	Diploma	135	41.8
	Degree and above	115	35.6
	Total	323	100.0
Working Experience	<5 years	133	41.2
	6 - 10 years	105	32.5
	>10 years	85	26.3
	Total	323	100.0

Table 2. Computerized Accounting system threats

no	threats	IS Component	source	Mean	Strongly disagree		Disagree		Neutral		Agree		Strongly agree		Std. Dev
					Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	
1	Accidental entry of bad data by employee	Input	Internal	3.44	11	3.4	45	13.9	109	33.7	106	32.8	52	16.1	1.03
2	Intentional entry of bad data by employee	Input	Internal	2.56	101	31.3	64	19.8	71	22.0	49	15.2	38	11.8	1.37
3	Employees sharing of password	Database	Internal	3.07	76	23.5	39	12.1	54	16.7	93	28.8	61	18.9	1.45
4	Unauthorized access of data or system by outsiders (hackers)	Database	External	2.76	86	26.6	65	20.1	64	19.8	56	17.3	52	16.1	1.43
5	Unauthorized access to the data and/ or system by employees	Database	Internal	2.71	84	26.0	71	22.0	65	20.1	61	18.9	42	13.0	1.37
6	Introduction (entry) viruses to the computer system	Process	External	3.50	24	7.4	29	9.0	89	27.6	123	38.1	58	18.0	1.11
7	Interception of data transmission from remote location	Process	Internal	3.19	27	8.4	47	14.6	119	36.8	97	30.0	33	10.2	1.07
8	Creation of fictitious or incorrect output	Process	Internal	3.14	32	9.9	61	18.9	100	31.0	90	27.9	40	12.4	1.16
9	Accidental destruction of data by employee	Process	Internal	2.92	47	14.6	68	21.1	104	32.2	73	22.6	31	9.6	1.18
10	Intentional destruction of data by employees	Process	Internal	2.67	88	27.2	71	22.0	67	20.7	54	16.7	43	13.3	1.38
11	Suppression or destruction of output	Output	Internal	3.24	27	8.4	41	12.7	124	38.4	91	28.2	40	12.4	1.09
12	Theft of data or information	Output	External	3.23	28	8.7	55	17.0	97	30.0	101	31.3	42	13.0	1.14
13	Unauthorized copying of output	Output	Internal	3.21	25	7.7	58	18.0	106	32.8	93	28.8	41	12.7	1.12
14	Printing and distribution of information by unauthorized persons	Output	Internal	3.18	36	11.1	52	16.1	100	31.0	87	26.9	48	14.9	1.20
15	Prints and distributed information are directed to people who are not entitled	Output	Internal	3.14	48	14.9	47	14.6	88	27.2	91	28.2	49	15.2	1.27
16	Unauthorized document visibility by displaying on monitors or printed on papers	Output	Internal	3.10	38	11.8	69	21.4	86	26.6	82	25.4	48	14.9	1.24
17	Sensitive document are handed to non security personnel for shredding	Output	Internal	3.05	52	16.1	46	14.2	102	31.6	79	24.5	44	13.6	1.26
18	Natural disasters such as fire or flooding		External	3.10	40	12.4	39	12.1	132	40.9	72	22.3	40	12.4	1.15
19	Human made disasters such as loss of power		External	3.02	46	14.2	46	14.2	125	38.7	69	21.4	37	11.5	1.18

3.2. Database

Three items were recognized under the category of database. Password sharing among employees is perceived as the highest threats in the category. But, most of respondent oppose to accept unauthorized access to database both from internal and external is considered as threats. This may reflect their perception towards the vulnerability of password hence may drive them to perceived, access from password sharing is the bigger threats for database.

3.3. Process

For process, five incidents were listed under this category. The most perceived threats is the external virus attack. But 44% form the respondent either disagree or neutral perceiving the incidents as a threat. This may trigger a concern to the management the level of perception of the user towards virus attack. Interception of data during transmission is perceived as the second threats in process. But data destruction by employees both intentionally or by accident were perceived as not a major threat. Not even 30% of the respondents agree on the statement and most of them choose neutral for it.

3.4. Output

Seven incidents were listed to be evaluated as threats to the government CAS. Destruction of output lead the rank as most respondent perceived it as the major threats to CAS. It is followed by theft of data/output and unauthorized copying of output, but still, more than 20% of the respondent did agree with this. More than 40% of respondents agreed that distribution of output to unauthorized and inappropriate recipient are among the threats to CAS. The least threats being perceived for out are unauthorizedly displaying the information on screen and also passing document for shtredding to inappropriate person. Nonetheless, more than 40% were agreed their CAS may face that incidents as threats.

3.5. Other Threats

The last two question is regarding the disasters caused both by human and nature. Though most of respondent choose neutral, but more than 40% agreed that these incidents may threats their CAS. Less than 30% disagree on the statement. This may due to their location which rarely involve in any natural disaster such as flood and earth quake. It also indicate that the user perceived other user as trustable and reliable.

3.6. Determinants of Perception Variations

There are some alarming issues in regards of the earlier findings. There are still some of the users view the listed threats as not a risk to the system. Hence, the study try to further explore the possibility of personal background to influence the respondents perceptions towards CAS threats. This is to test the hypothesis developed:

H_1: personal background is the factor for the variations of perceptions of CAS security threats.

Collected earlier there were six categories to represent the personal background of the respondent, namely age, gender, job level, working experience, educational level/background and department, which was group between staff from IT department and staff from non-IT department.

Through Pearson Correlation Coefficient, only educational background have a significant relationship with the perception of threats, r=0.046, p(2-tailed) <0.05. since, there are huge gap between the number of respondent in the vategory of department, by using the SPSS software, the study had randomly choose 46 respondent from the non-IT department to match with the IT department. The statistical result shows, there is no significant relationship between different department towards the perception of CAS threats (p>0.05).

To further explain the how strong does educational background may explain the variations of perception on threats, the study applied multiple regression analysis. The result shows educational background (β=.11, p<0.05) is the factor for differences on the threats perception. But, it only contributed a small portion of the explaination (R^2=1.2%). There are other factors that may be able to explain this variations and it is open for future research. So, the hypothesis is rejected and it is statistically concluded that personal background is not be the major factor of this variation of perceptions.

Table 3. Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.111	.012	.009	16.46254

4. Conclusions and Future Research

The article delivers an exploratory overview of the perceived degree of computerized accounting system security threats in Malaysia particularly in Jabatan Akauntan Negara Malaysia. As there is limited prior academic research on CAS threats in Malaysia, this research may provide an insight of perceive information system threats especially in computerized accounting environment. This may benefited the regulators and service providers on the threats issues and may trigger the awareness to improve their system security.

Through 19 computerised accounting threats listed for evaluation in the survey question, the findings reveal that most of CAS security threats are originated by the internal source which is the employees. In overall, from the dimensions of information system perspective and disasters caused by both human and nature, the respondent perceived them as threats to the CAS. Nonetheless the service provider and the sector should pay more intention about this issue as the highest score on the perception of the threats goes to neutral. A further investigation might be appropriate to evaluate the underlying reason for the perception. Among

the possible reason could be the degree of exposure towards the type of threats that might be faced in the computerized system environment, as discussed by[17], which highlights about the lack of training among employees may lead to misunderstand and misuse of the system.

Another point to highlight is the degree of understanding on the seriousness of virus attack as threats. There are still some of the respondent perceived it as not contributing any risk to the system, a extensive exposure about the cost and effect of the attacks may be appropriate.[18]. Highlighted the losses faced as the result of the attack.

Opposing the result gathered by[4], natural and human made disaster was found to be the least threat perceived among the user. Another least threats perceived are also theft of data and intentional entry of bad data of employees.

The study also prevail that personal background is not the factor contributing to the explaination of the variations of perception on CAS threats. Of all six categories, educational background only could explain 1.2% of this variation. Hence, there are still huge room for potential future research to be undertaken. Researchers may be interested to investigate the factors that may influence the user pereception on threats in order to contribute better understanding on required training to user. Apart of that, the caused and effect research may be appropriate to measure the effect of the threats perception towards the actual incidents happen. The future findings may produce a sound suggestion on type of security features need to be inculcated in a computerized accounting system.

As this research is only focus on the user of GFMAS in Jabatan Akauntan Negara Malaysia located in Putrajaya, this findings may not reflect the whole user of GFMAS nationally, and the general user of any computerized accounting system in Malaysia. widening the scope of respondent type and location might give a more insight and further support this findings.

ACKNOWLEDGEMENTS

The authors would like to wish a special thanks to the staffs of Jabatan Akauntan Negara Malaysia in Putrajaya who had kindly participate in this survey. Also special thanks to our dearest students who had assist us in the data collection process.

REFERENCES

[1] Zakariah Salleh.(2007). International Review of Business Research, Malaysian Governmental Accounting: National Context and Users Orientation. Papers,3 (2),376-384..

[2] Jabatan Akauntan Negara Malaysia. Online available at: http://www.anm.gov.my/main

[3] Abu-Musa, A.A. (2006). Journal of Information System Perceived security threats of computerized accounting information system in the Egyptian banking industry, 20(1), 187-203.

[4] Davis, C.E. (1997), The CPA Journal, New York, An assessment of accounting information security, NY, Vol. 67 No. 3, pp. 28-34

[5] Ryan, S.D. and Bordoloi, B. (1997), Information & Management, Evaluating security threats in mainframe and client/server Environments, Vol. 32 No. 3, pp. 137-42.

[6] Siponen, M.T. (2000), Information Management & Computer Security, A conceptual foundation for organizational information security awareness, Vol. 8 No. 8, Bradford, pp. 31-44.

[7] Dhillon, G. (1999), Information Management & Computer Security, Managing and controlling computer misuse, Vol. 7 No. 4, pp. 171-5

[8] Abu-Musa, A.A. (2007), Information Management & Computer Security, Evaluating the security controls of CAIS in developing countries: an empirical investigation, Vol. 15 No. 2, pp. 128-14

[9] Dhillon, G. (1999), Information Management & Computer Security, Managing and controlling computer misuse, Vol. 7 No. 4, pp. 171-5

[10] Ernst and Young (2004). Ernst and Young Global Information Security Survey 2004. Online available at: http://www.ey.com

[11] NISER (2004). NISER ICT Security Survey for Malaysia 2004. Online available at: http://www.niser.org

[12] MYCERT incident Statistics, online available at: http://www.mycert.org.my

[13] McAdams, A. C. (2004). Information Management Journal, Security and risk management: A fundamental business issue, pp. 36−44

[14] Spathis, C. (2004). Business Process Management Journal, Enterprise resource planning systems' impact on accounting processes, Vol. 10 No 2, pp 234-247.

[15] Abu-Musa, A.A. (2006). Managerial Auditing Journal, Exploring perceived threats of CAIS in developing countries: the case of Saudi Arabia. 21(4), 387-407

[16] Beard. D and Wen.H.J. (2007). Information Systems. The CPA Journal Reducing the Threat Levels for Accounting, 34

[17] Wright, S. and Wright, A. (2002), Journal of Information Systems, Information system assurance for enterprise resource planning systems: implementation and unique risk considerations, Supplement, Vol. 16, pp. 99-113

[18] Brynes, C. (2005). The Gartner Group: Information Security Trends 2005–2007. Online available at: http://www.gartner.com