ACCOUNTING INFORMATION SYSTEM SECURITY: A SURVEY OF E-COMMERCE COMPANIES IN MALAYSIA

[1]Raja Haslinda Raja Mohd Ali and [2]Rafeah Mat Saat
Faculty of Accountancy
Universiti Utara Malaysia, 06010 Sintok, Kedah
[1]rj.linda@uum.edu.my and [2]rafeah@uum.edu.my

Abstract: The reliance on information and rapidly changing technology in Malaysia has forced organizations especially in e-commerce industry to implement comprehensive information security programs and procedures to protect their information assets. Failure to secure information or to make it available when required to those who need it can, and does, lead to financial loss. Professionals and managements should realize the importance of having secured system. In recent years, the cases of computer fraud, hackers and computer crime is unavoidable unless stringent protections being implemented. Tremendous increase in computer related fraud in Malaysia business organizations would reduce the confidence of the shareholders towards companies. This paper intends to identify the significant security breaches that actually faced by the computerized accounting systems in e-commerce industry. It also investigates the controls to prevent and detect security breaches that have been implemented in this industry.

Keywords: Computer security, E-commerce, Accounting information system

INTRODUCTION

In Malaysia, the reliance on information and rapidly changing technology have forced organizations especially in the e-commerce industry to implement comprehensive information security programs and procedures to protect their information assets. Failure to secure information or to make it available when required to those who need it can, and does, lead to financial loss.

Few studies have been done on the accounting information system security especially in e-commerce industry. In 2000, Ahmad [1] investigated the main threats that may face the computerized accounting systems security, and the prospective controls that are implemented in the Egyptian bank to prevent and detect security breaches. His study shows that most significant perceived security threats are accidental entry of bad data by employees, accidental destruction of data by employees, unauthorized access to data or system by outsiders, theft of data and information, and direction of some prints and computer output to individuals not entitle to receive it.

While Basariah et al. (2000) [2] examined the scope of computer crime and the existing policies and procedure relating to the system security in financial institution. Their study shows that financial institutions in Malaysia did experience the computer crime such as unauthorized access. These institutions are aware and have taken several steps regarding the securities policy and procedures in their system.

The objectives of this research are as follows:

- To identify the potential security threats to the computerized accounting systems in the Malaysia e-commerce industry.
- To investigate the controls that has been implemented in the Malaysia e-commerce industry to prevent and detect security breaches.

MATERIALS AND METHODS

Respondents

This study focuses primarily on companies associated with e-commerce services. The study respondents consist of all registered e-commerce service provider under Multimedia Development Corporation (MDC) located in Malaysia. MDC was established by the government of Malaysia to spearhead the development and implementation of the Multimedia Super Corridor (MSC). From MDC website as at June 2003 there are 91 companies that that have been categorized under E-Commerce Service Provider.

Research instrument

A survey questionnaire approach has been used to obtain the data for this study. We adopt a set of questionnaire designed by Basariah et al. (2000) [2] with some modification to suit the study.

The survey instrument is divided into three sections. Part 1 is on company profile including type of company, size of the company (number of employees), and the percentage of employee that use computers and Accounting Information System (AIS) software used. Part 2 contains questions about potential security threats in e-commerce companies, which will answer the first objective of the study. Meanwhile, Part 3 contains question about prevention and detection of security breaches that apply in e-commerce companies. This part covers the infringement detection and monitoring, security incidents, incidence response and security policy of the company. The respondents are also asked on their awareness of Cyber Laws implemented in Malaysia.

Data collection

A set of questionnaire was sent to the manager of information technology of the respective e-commerce company, who is considered to be the most appropriate respondent. To ensure prompt reply, the questionnaire was addressed to the person in charge of IT in the company.

Data analysis

A descriptive analysis is mainly used in this study, which includes frequency distribution and means score of the variables.

RESULTS AND DISCUSSION

Demographic Factors of the Respondents

The summary of the respondent background could be depicted in Table 1. It could be seen that 44.4 percent of the respondent are developer as well as consultant of their companies' software and applications. 33.3 percent are e-commerce service providers while most of these e-commerce companies showing less than 40 employees.

Table 1: Demographic Factors of Respondents

Variables	Frequency		Mean
	N	(%)	
Type of company			
Developer and consultant of software and applications	8	44.4	
E-commerce service provider	6	33.3	
Developer of online travel services	1	5.6	
Online payment service provider	4	22.2	
Provider of IT outsourcing	2	11.1	
Internet adviser	1	5.6	
Provider of e-commerce supply chain	4	22.2	
Portal developer	2	11.1	
Provider of financial portal	1	5.6	
Others	2	11.1	
No. of employee			1.89
1-20	8	44.4	
21-40	6	33.3	
41-60	2	11.1	
>60	2	11.1	
No. of computer			2.33
1-20	3	16.7	
21-40	8	44.4	
41-60	5	27.8	
>60	2	11.1	
Percentage use of computer			8.22
41-50%	1	5.6	
51-60%	2	11.1	
81-90%	1	5.6	
91-100%	14	77.8	

Most of e-commerce companies surveyed have 21 to 40 computers. 77.8 percent of the respondents claimed that their employees make use of 91 to 100 percent of computer work everyday. This is common for e-commerce companies because according to IATFEC (Inter Agency Task Force on E-commerce) refers to all forms of business transactions conducted over public and private computer networks. However, only 16.7 percent admitted that they use less than 50 percent of computer work daily.

Potential Security Threats

Table 2 exhibits the potential security threats faced by e-commerce companies surveyed. A large percentage of respondents (83.3 percent) acknowledge that accidental destruction of data by employee is the main threats for AIS. Second, is the accidental entry of bad data by employee (66.7 percent), third is employee sharing passwords (61.1 percent) and lastly unauthorized distribute of data (61.1 percent). Finding also lists the potential threats, which will give impact on e-commerce companies over the next five years. The most popular threats is hacking showing 88.9 percent, followed by intellectual property offences, 55.6 percent, greater use of encryption at 44.4 percent and information warfare at 44.4 percent.

Table 2: Potential Security Threats

Variables	Frequency	
	N	(%)
AIS security threats		
Accidental entry of bad data by employee	12	66.7
Accidental destruction of data by employee	15	83.3
Employees sharing passwords	11	61.1
Unauthorized distribute data	11	61.1
Security threats for next 5 years	16	88.9
Hacking	5	27.8
Theft	7	38.9
Fraud	5	27.8
Forgery	8	44.4
Greater use of encryption	10	55.6
Intellectual property offences	6	33.3
Use of false identities	8	44.4
Information warfare		

Prevention and Detection of Security Incidents

Table 3 shows that 100 percent of e-commerce companies routinely conduct system security audits. 33.3 percent conduct security audits more than 6 months, followed by 3 to 4 months (27.8 percent), 1 to 2 months (22.2 percent) and 5 to 6 months (16.7 percent). The mean for routine security audit is about average, which are 2.61 on a 4-point Likert scale.

For the security incident, out of the 18 e-commerce companies, only one company denied that their company experienced unauthorized use of its computer systems within the last twelve months. 7 respondents or 41.2 percent experienced 1 to 5 incidents within twelve months, 5.9 percent experienced 6 to 10 incidents, 41.2 percent answered 'None' and 11.8 percent answered 'Don't Know'. The mean of 3.29 on a 6-point Likert scale indicates that most of the respondents experienced 1 to 5 security incident within twelve months.

Results also shows that 100 percent of the respondents agree to patch their security holes as an action taken when experienced computer intrusion. Only 5.6 percent declared that they report to anyone outside organization and update their security policies when faced with computer intrusion, whilst 16.7 percent and 11.1 percent will report to law enforcement agency and external response team respectively.

Surprisingly, only 77.8 percent of e-commerce companies agreed to make report if their security system is being attacked. Malaysia Royal Police and MIMOS would be their choices, showing about 50 percent and 44.4 percent respectively.

Table 3: Prevention and Detection of Security Incidents

Variables	Frequency		Mean
	N	(%)	
Routine security audits			2.61
1-2 month	4	22.2	
3-4 month	5	27.8	
5-6 month	3	16.7	
> 6 month	6	33.3	
Security incident within 12 months			3.29
1-5 incidents	7	41.2	
6-10 incidents	1	5.9	
None	7	41.2	
Don't know	2	11.8	

Cont'
Table 3: Prevention and Detection of Security Incidents

Action taken when experienced computer intrusion			
Patch security holes	18	100	
Report to anyone outside organization	1	5.6	
Report to law enforcement agency	3	16.7	
Report to external response team	2	11.1	
Other-Update security policies	1	5.6	
Would respondents report when being attack?			
Yes	14	77.8	
No	4	22.2	
To which agency?			
State territory	2	11.1	
Malaysia Royal Police	9	50.0	
Mimos	8	44.4	
Have written policy?			0.67
Yes	12	66.7	
No	6	33.3	
Have procedure for preserving evidence?			0.42
Yes	5	41.7	
No	7	58.3	
Have provision for notifying law authorities?			0.42
Yes	5	41.7	
No	7	58.3	

It is also shown that 66.7 percent of the organizations have a written policy on security and misuse of computing facilities. But, only 41.7 percent of the policies include procedure for preserving evidence for civil or criminal proceeding after a security breach. Furthermore, 41.7 percent have provision for notifying appropriate law enforcement authorities of breaches.

Security Threats

E-commerce companies in Malaysia do experience the accounting information system threats. The most significant threat is represented by the highest percentage showing 83.3% of the security threats are from accidental destruction of data by employees, followed by accidental entry of bad data, employees sharing password and unauthorized distribute data. This finding is consistent with previous studies by Ahmad (2000) [1], who also highlighted that the significant security threats are accidental destruction of data, accidental entry of bad data, sharing passwords and unauthorized distribute data.

Apart from this, the security threats for the next five years show that hacking will be the top most lists of threats, which is similar to a finding by NISER – National ICT Security and Emergency response Center (2004) [3].

Prevention and Detection of Security Threats

Base on Swanson (2000) [4], it is pointed that routine, independent review of security system and procedures is important to ensure that organization has protection and confirm that they are working as designed. Results have revealed that all the respondents did conduct a system security audit. However, for companies that conduct their security audit between 1 to 2 months, they reported that they did not experience any unauthorized use of their systems within 12 months. Unlike those companies that conduct security audit less frequently, which is within 12 months they did experience the unauthorized used. This scenario may be due to the frequent routine security audit.

Another prevention of security incidents is security policy, where every company should have their own security policy to provide the guidelines on how to control the information technology. Failure to have the policy will result in employees not knowing how to control it or who to report to in case of security breaches. This finding shows that only 66.7 percent with security policy and 41.7 percent without a complete security policy where some of them do not have the procedure for preserving evidence and provision for notifying law authorities. As a result, the incidents happen will remain incidents where there is no action taken to control it.

Future Research

E-commerce companies have always been the target for information system threats. Whether they realize or not, the routine security audit and other controls that they have implemented to protect their valuable assets, have prevented them from being the victim of information intrusion and destruction. Even though, some companies may not have their written policy on computer and information system, it is hoped that this finding would show them the importance of having this policy.

Therefore, it is suggested that future research will identify the reasons why e-commerce companies do not report their security incidents and why security policy is not a compulsory for e-commerce companies.

REFERENCES

1. Ahmad A. Abu Musa, (2000), Computer crimes: How can you protect your computerized accounting information system?, *Journal of American Academy of Business*, Cambridge, Sep 2002.

2. Basariah S., Mahamad, T., & Shamharir A., (2000), Computer Crime and Security: a survey of financial institutions in Malaysia.

3. National ICT Security and Emergency Response Centre, (2002), NISER Incidents Statistics, Retrieved April 3, 2004, from http://www.niser.org.my

4. Swanson, D. (2000), Secure Strategies, *Information Security Magazine*, Retrieved April 1, 2004, from http://infosecuritymag.techtarget.com/