Computer Crime and Security:
A survey of Financial Institutions in Malaysia

By:
Basariah Salim, Mahamad Tayib, Shamhahrir Abidin
School of Accountancy, Universiti Utara Malaysia
06010 UUM,Sintok
Kedah

Presented at:
ETEC 2000
Hilton Hotel

Presented on:
21-23 November

Computer Crime and Security:
A survey of Financial Institutions in Malaysia

Abstract

As the world moves towards a virtual age, the increasing use and reliance on computers can not be avoided. Indeed, the use of computers has touched every aspect of life of people around the world. On the other hand, computer technologies also have ability to destroy those benefits if they are wrongly used to gain unethical advantage from these technologies. Studies in United States of America, Europe and Australia show that computer crime has grown along with the increase in the use of computers. Considering the alarming growth figures of computer crime around the world, it is believed that Malaysia too is also experiencing similar problems. So, this study is attempts to determine the scope of computer crime in Malaysian financial institutions as well as raise the level of security awareness. The results will potentially provide us with better understanding of the threats as we gathered the database.

Computer Crime and Security in Malaysia: A survey of Financial Institutions

Introduction

As the world turns to the information age, the increasing use and reliance on computers cannot be avoided. Indeed, the use of computers has touched every aspect of life of the people around the world. The use of computers, undoubtedly, has contributed great benefits not only to businesses, economies, industries and government but also to human life itself. For instance, more and more people nowadays depend on computers for medical treatment and every day people communicate with each other through computer.

Realizing the need of computer technologies in developing the country, Malaysia has established the Multimedia Super Corridor (MSC) to help companies of the world test the limits of technology and prepare them for the future. The MSC brings an integrated environment with all the unique elements and attributes necessary to create the perfect global multimedia. This includes investing in an environment that encourages innovation, helps companies, both Malaysian and international, to reach new technology frontiers, partnering global IT players and providing the opportunities for mutual enrichment and success. Seven primary areas for multimedia applications have been identified. The applications include electronic government, multi-purpose card, smarts school, telemedicine, research and development cluster, worldwide manufacturing webs and borderless marketing.

However, the use of computers and its technology has also raised the question of security. As depicted from United Nation Commission on Crime and Criminal Justice's (1995) manual on the prevention and control of computer-related crime:

> The burgeoning of the world of information technology has, however, a negative side: it has opened the door to antisocial and criminal behaviour in ways that would never have previously been possible.

Further, the commission warns that the consequences of computer crime may have serious economic costs as well as serious costs in terms of human security.

As evidenced by researchers, computer crime grew rapidly with the increase use of computers in every day activities (CSI: 1998, Thompson: 1998, Carter and Katz: 1996). Most of companies and organizations in the world are afraid of this crime because it brings a lot of problems to companies. Companies are not just suffering from financial losses (taken by hackers and recovery costs) but also may have to stop operation due to the intrusion. The reason is that, beside stealing the money, some of the hackers are interested in intellectual property which includes such things as new product plans, new product descriptions, research, marketing plans, prospective customer lists and similar information which are kept in companies' computers. Furthermore, the hackers can anytime break-in into an organisation's system including the one that has a very sophisticated security system as what happened to Pentagon where a young Israeli hacker infiltrated into their computer's system in February 1997 (McCune: 1998).

The intruders can be anybody and from anywhere in the world. For example, in 1994, Russian hacker with a lap top computer, sitting in an apartment in St. Petersburg, Russia, intruded into

Citibank computer system in New York and illegally transferred $10 million to himself (McCune: 1998). With the use of worldwide networking, organisations are now not only facing threatening from hackers in their own country but also from foreigners.

Considering the alarming reported figures of computer crime around the world. It is believed that Malaysia is also experiencing this sort of situation. However, as far as this study is concerned, no survey or research has been done on this issue and consequently, left some questions unanswered. The questions such as:

- what type of computer crime is happening in Malaysia
- are our companies and government especially the Law enforcement agencies ready to face and cope with this crime in the future?
- to what extent are companies ready to prevent computer crime from happening?

are of interest before the maximum implementation of IT in business can be done.

Companies must ensure that, their systems are well equipped with proper security countermeasures such as encryption, operations security, cash account security, employee training and firewall. In addition, law enforcement agencies must be prepared to deal with this matter since it is hard to get evidence for this kind of crime. Besides experience in investigating, they must possess knowledge on computer technologies. Furthermore, it is really necessary to ensure that, Malaysian cyber law acts (namely Computer Crimes Act 1997, Digital Signature Act, 1997 and Copyright Act 1997) cover every aspect of this crime.

Computer Crime

Computer crime still has no precise definition although it is used in many studies. Commonly, the term "computer crime" is often used interchangeably with "computer-related crime". There has been a great deal of debate among experts on what constitutes a computer crime For instance, Moscove (1997) in his book, Core Concepts of Accounting Information System wrote that computer crime is a misnomer since it is not the computer that commits crimes, but people. He suggested that computer-assisted crime term is probably a better descriptor of computer crime.

Meanwhile, the United States Department of Justice defines computer fraud as any illegal act for which knowledge of computer technology is essential for its perpetration, investigation or prosecution. More specifically, Romney (1997) elaborated that computer fraud includes the following:

- Unauthorised use, access, modification, copying, and destructive of software or data.
- Theft of money by altering computer records or the theft of computer time
- Theft or destruction of computer hardware
- Use or the conspiracy to use computer resources to commit a felony
- Intent to illegally obtain information or tangible property through the use of computers

Several studies have been carried out in the area of computer crime. Most researchers agree that the extent of computer crimes appears to be expanding rapidly. A study conducted by the American Bar Association (ABA) in 1987 found that of the 300 corporations and government agencies questioned, 72 respondents (24 percent) claimed to have been the victim of a computer-related crime in the twelve months prior to the survey. The combined estimated losses

from these crimes ranged from $145 million to $730 million over the 1-year period (U.N: 1995).

In 1989, the Florida Department of Law Enforcement (FDLE) surveyed 898 public and private sector organizations that conducted business by computer. Of the 403 respondents, 25 percent reported they had been victimized by computer criminals (U.N: 1995) The study found that embezzlement of funds by employees to be a major source of the crimes.

Another study, which had been carried out by the United Nations Commission on Crime and Criminal Justice, surveyed 3000 Virtual Address Extension (VAX) sites in Canada, Europe and the United States in 1991 to assess computer security threats and crimes. The results showed that 72 percent of the respondents reported a security incident within the previous months, with 43 percent reporting the incident was criminal in nature (U.N: 1995). Security threats came most often from employees or other people with access to the computers. However, respondents reported a number of external breaches from hackers telephoning into the systems or accessing via network

In 1996, David and Carter (1996) found a trend of victimization that increased significantly over previous studies, with 98.5 percent of the respondents reporting they had been victimized and 43.3 percent admitting to being victimized more than 25 times. Consistent with previous studies, employees committed most of the reported crimes.

Beginning from 1996 Computer Security Institute (CSI) together with Federal Bureau of Investigation (FBI) International Computer Crime Squad's San Francisco office of United States conducted their annual survey on computer crime and security. A survey in 1997 reported relatively serious break-ins, where the total losses in 1997 were nearly $1.37 million, a 36 percent increase from the previous year. Through 1997 survey, they found that an intensive used of Internet in today technology has also contributed to the increment of this crime. The number of organizations that cited their Internet connection as a frequent point of attack rose from 37% in 1996 to 47% in 1997. Furthermore, in 1997 survey, 43% of the respondents reported inside breaches and 47 percent outside breaches. These responses indicate the "conventional wisdom" that 80 percent of information security problems are internal is no longer true (U.N: 1995, Carter and Katz: 1996).

Meanwhile, a survey conducted by Thompson (1998) showed that, the main threat to Australian companies from computer misuse is still from within their own organization. However, the researcher anticipates that an external threat will increase in the future since respondents clearly identified "hacking or systems intrusion" as the issue "most likely to impact on their organizations in the future". Surveys that conducted by Thompson (1998) and Carter and Katz (1996) reported that, financial institutions are a favourite sector for intrusion.

Research Objectives

The primary purpose of this study is to identify and examine the extent of computer crime in financial institutions. The financial sector is of interest as it was reported as the most affected industry (CSI, 1998; Thompson, 1998 and Carter and Katz, 1996). Specifically, this study is aimed:

- To identify and examine the nature and scope of computer crime in financial institutions.
- To identify and examine existing policies and procedures relating to system security.
- To identify and investigate the level of awareness among IT managers towards computer security system in financial institutions.

Research Significance

This study attempts to determine the scope of computer crime in the Malaysian financial sector as well as raise the level of security awareness. The results will provide us with better understanding of the threats as we gather the database. In addition, the findings of this study will be useful especially for financial institutions in planning their action toward system's security in order to prevent computer crime. It will also be helpful for law enforcement agencies in dealing with this threat more effectively and subsequently, to provide a better service to their clients and public.

Methodology

The survey was designed to collect data from a representative spread of financial institutions throughout Malaysia. This sector is chosen because it was determined as a popular place for intrusion from the previous researches (Thompson; 1998, Carter and Katz; 1996). A total of 123 financial institutions listed in The Kuala Lumpur Bankers Directory 1998/99, which is issued by Arab-Merchant Bank Berhad, have been taken into consideration. The financial institutions consist of commercial banks (37), merchant banks (12), finance companies (39), discount houses (7), development banks/finance institutions (8), money brokers (8) and other financial bodies (12). A set of questionnaire, which is replicated from Thompson (1998), was used in collecting data. The questionnaire was sent to the information manager or corporate security professionals, who are considered the most appropriate respondents to answer this. In order to encourage prompt reply, every questionnaire was personally addressed to the recipient identified earlier.

Descriptive analysis will be used to analyse the data collected. These include analysis of the results disclosed by tables of: (1) frequency distribution; (2) measuring location (i.e. Mean scores of the variables); and (3) measuring dispersion (i.e. standard deviations).

A total of 123 questionnaires have been sent out. This number represents seven categories of financial institutions, which are commercial banks, merchant banks, finance companies, discount houses, money brokers, development banks and other financial bodies. Unfortunately, seven (7) questionnaires have been returned due to address changes and surprisingly, 1

questionnaire was returned because the organization's system was not computerised yet. So, just 116 organizations were effectively surveyed in this study. A total of 35 questionnaires were returned (30.17%), where, some of the questionnaires were improperly completed. However, according to Carter & Katz (1996), this returned rate is considered sufficient in performing descriptive analysis although they were improperly completed. Their research also showed a returned rate around 30.5% out of 600 samples. Research which done by Thompson (1997) in Australia showed a high rate of returned which was around 52.92 % out of 310 organizations.

Descriptive Analysis

Organization Profiles

Table 1 shows the response of the respondents towards the questionnaires sent to them. Highest response rate came from commercial banks and finance companies (26.47% and 23.53%). Meanwhile, table 2 and figure 1 show a number of employees in companies surveyed and their annual turnover.

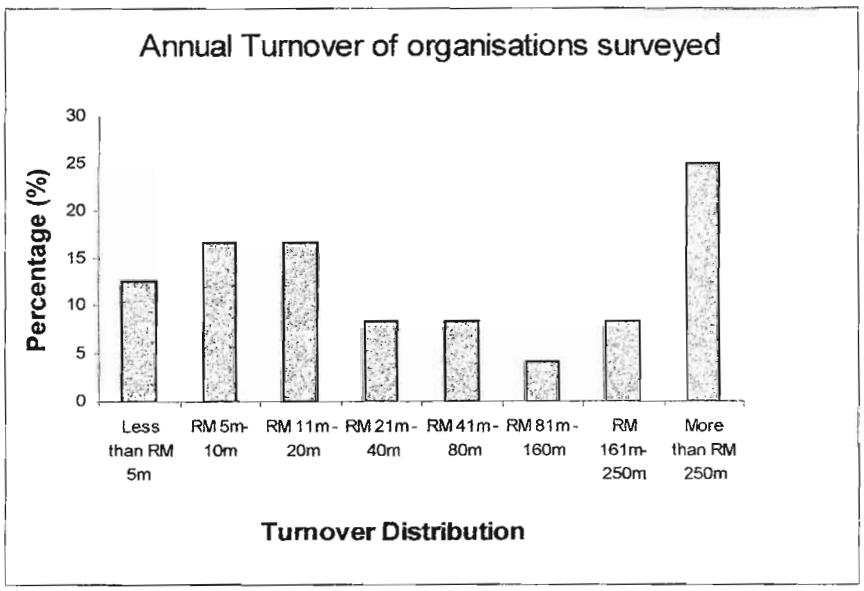
Table 1
Questionnaire Response Rate

Organization	QA Send	Reply Rate(%)
Commercial bank	37	26.47
Merchant Bank	12	14.71
Finannce Company	39	23.53
Discount House	7	2.94
Money Broker	8	2.94
Development Bank	8	8.82
Other Financial Body	12	20.59
Total	123	100

Table 2
Number of Employees of Organisations Surveyed

Distribution	% of respondents
Less than 100	34.38
100 to 500	34.38
501 to 1000	0
1001 to 2000	21.85
2001 to 3000	0
3001 to 4000	3.13
4001 to 5000	3.13
5001 to 10000	3.13
more than 10000	0
Total	100

Figure 1



Computer Environment

70% of respondents claimed that their employees make use of 80-100% of computers everyday (figure 2). All respondents reported that their computer systems are inter-networked, where 48.57% of 35 respondents are corporate local area network, 42.86% are corporate wide area network and 8.57% are corporate global area network (figure 3). In addition, 91% of the companies provide corporate access to the Internet.

Figure 2

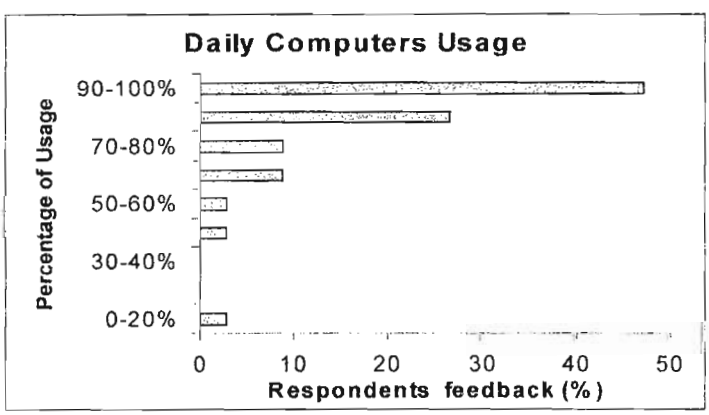
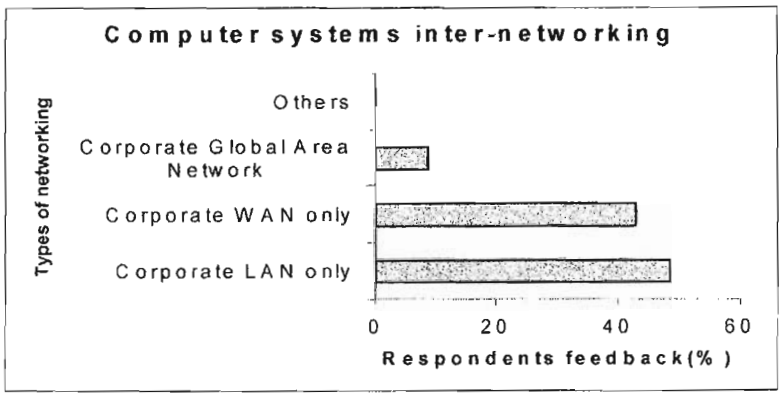


Figure 3



Risk Assessment and Risk Management

Table 3 (appendix) exhibits the risk assessment and risk management policies of companies surveyed. 22 respondents, or 73.33% answered 'Yes' to the question whether their organization has performed a qualitative and/or quantitative risk assessment to determine the specific areas of potential risk that could impact their ability to perform day-to day business functions. Accordingly, 20% answered 'No' and followed by 6.67% on 'Do Not Know'. On the other hand, 67% said that risk assessment results have been prioritised to facilitate budget allocations, 25.9% said 'No' and 7.1% 'Do Not Know' about this question.

Eighty-four of respondents said that their organizations have a written policy on the security and misuse of computing facilities. Of these, 69% answered that their organization written policy includes how to deal with network intrusions. Moreover, 67% of the policy includes sanctions/procedures for dealing with breaches. Beside that, only 42.3% of the policy includes provisions for notifying appropriate law enforcement authorities of breaches. Of these, 46% answered 'No' and 11.7% 'Do Not Know' whether their organization have the policy or not. Unfortunately, for the question whether their organization have any policy or procedures for preserving evidence for civil or criminal proceedings after a security breach in which valuable information has been compromised, only 30% out of 30 respondents said 'Yes', 63% of these answered 'No' and 7% 'Do Not Know'.

The survey found that 73.3% out of 30 respondents answered that their organization have a computer security awareness programs for all employees using information technology. Interestingly, 96.8% out of 32 respondents mentioned that their organisations instruct their employees in the ethics of using computers. However, only 21.2% out of 33 respondents reported that most of their employees with access to computer and telecommunications system have a working knowledge of the current laws on misuse of computer systems. Of these, 72.79% reported a few and 6.1% none. This means that less than one third of the users are not exposed nor have knowledge in current laws.

Police department has been identified, as a major choice of law enforcement agencies which will be contacted in the event of an accident. Some of the respondents will contact Bank Negara Malaysia, Securities Commission, lawyers, and MIMOS. The main reason for contacting a law enforcement agency is because of company policy. The next reason is to

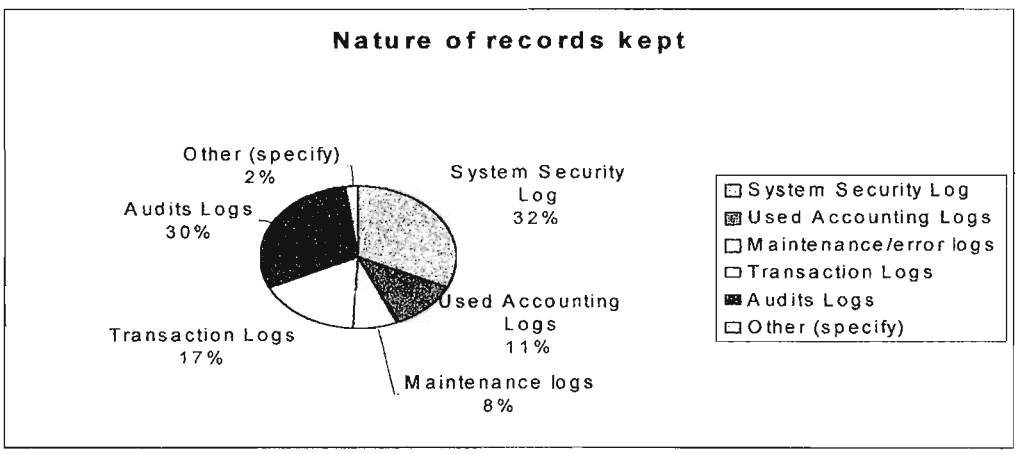
prosecute offender and the third reason is to recover costs/damages and for assistance in tracing offenders. The rest are to make an insurance claim, to prevent further victimization, public image, retribution and civic duties.

More than two thirds of organizations that participated in this survey do not maintain liaison with law enforcement agencies regarding misuse or unauthorized access of computer systems. Only 17.2% maintain the liaison. Of these, they liaisied with police department, Bank Negara Malaysia, MIMOS and Securities Commission. The main reason for not liasing with law enforcement was that incidents occurred too infrequently to require regular liaison. The other reasons are all action taken is of civil nature, do not know who to contact, too busy and others.

Infringement Detection and Monitoring

The finding shows that, 90% out of 31 organizations routinely conduct system security audit. 86% of these maintain historical records/data of systems misuse or intrusion attempts. The details of how they maintain the records/data are shown in Figure 4.

Figure 4



Security Incidents (attacks/intrusions)

Out of 31 respondents, only 25.8% acknowledged that their organization experienced unauthorized use of its computer systems within the last twelve months. All of those that had experienced unauthorized use had identified five or fewer separate incidents. Most of the intrusions were from inside the organization. However, there were also reported intrusions from outside. Unauthorised access had been recognized as a most favourite way of attacking an organization's systems. Of these, 50% (4 respondents) estimated either the direct or indirect costs to their organizations of this misuse as under RM10, 000.00 per incident. The remaining 50% claimed that no costs were incurred in the incident.

31.5% of the respondents who acknowledged that their system had been intruded had identified a pattern in the type of information accessed. Those that answered "Do Not Know" were having a problem in identifying the pattern. Financial systems/data has been identified as the most of type of information accessed. The rest are confidential corporate data, intellectual properties, personnel information and others. Internal systems were identified as the most

frequently attacked access point. It was followed by the Internet access. The disgruntled employee was identified as the most likely source of breach. The next largest source of groups was criminal. The third largest was independent hackers or info brokers. The rest, which are competitors, customers, suppliers, foreign governments, were not viewed as the high-risk groups.

Incidence Response

Nearly half of 23 respondents, i.e. 47.83%, will do their best to patch security holes in their system. Reporting the incident to a law enforcement agency and solicitor to seek civil remedy are place as the second choice of their reaction towards the intrusion. Financial gain was seen as the main motivation for attempting to breach computer systems, followed by curiosity and espionage.

Fear of losing customers was given as the main reason for not having to seeking help from law enforcement agencies. This was followed by fear of further exploitation/intrusion and for the short measure internal disciplinary actions were taken. By the way, 29.73% out of 37 respondents were willing to report computer related crime incidents to a law enforcement agency if they have a chance of recover the losses. 21.62% will immediately report when detected and 18.92% will report if mandatory by law.

The survey shows that only 22.6% (7 respondents out of 31) have received advice from law enforcement agencies on the vulnerability of information stored on computer systems. Unfortunately, 70.96% did not receive any advice and 6.44% do not know about this information. 45.71% of respondents will refer to private consultants for advice on computer crime/incidents. The second closest is their own staff (25.71%) and followed by law enforcement (14.29%) and others (14.29%) as a third choice.

When asking whether they would find it useful to receive information on computer crime (for example types of crime, ways to prevent and what to do if you are victimized) from law enforcement, 93.5% answered yes. They prefer to receive the information in pamphlet (29.58), email list (25.35), presentations (21.13%) and Internet (18.31%). Table 4 lists a several factors, which will increasingly impact on organisations over the next five years.

Table 4
Factors Which will increasingly impact on organisation

Factors	No. Of respondent
hacking and use of malicious code	14
theft	2
fraud	15
forgery	12
theft of telecommunications services	8
greater use of encryption	16
intellectual property offences	6
electronic extortion	5
money laundering	3
cash theft and counterfeiting	2
virtual company crime	8
use of false identities	12
emergence of 'black' information-markets	2
shift from conventional crime against property to computer related offences	8
increase in virtual crimes (data rape, email harassment, flaming, etc)	12
information warfare (e.g. Commercial sabotage and espionage, cyber terrorism, etc)	5
emergence of organized crime groups operating extensively over networks	6
other (specify)	0

Discussion and Summary

This section discusses the above findings and compares with other studies that have been done by others in order to highlight the extent of the computer crimes in Malaysian financial institutions.

Nature and Scope of Computer Crime

As being discussed in the literature, United States Department of Justice defines computer fraud as any illegal act for which knowledge of computer technology is essential for its perpetration, investigation or prosecution. It means that, any crime or fraudulent incident can only be categorized as computer crime if the incident happened with the use of computer. However, the computer cannot commit the crime on its own. People misuse the computer to achieve their own interests.

There are five types of computer crimes namely fraud by computer manipulation, computer forgery, damage to or modifications of computer data or programs, unauthorized access to computer systems and service and unauthorized reproduction of legally protected computer programs (U.N: 1995). So, if we refer to the definition and types of computer crimes above, we can only conclude that computer crime can be avoided if we live without computers. But, in the electronic era, we cannot run away from computers and their technologies. Survival of companies in the future depend very much on knowledge or information that they have, where it can be sustained through computers and it technologies. Recently, commercial banks for example Maybank, Phillio Allied and HSBC are heavily competing with each other to provide an online service known as electronic banking to their customers. So, in order to survive and operate in this electronic environment, financial institutions have to ensure that their system are highly guaranteed safe not just from their side but also for their customer. If not, they are exposing themselves to a computer crime threat. According to a survey which was conducted biennial by KPMG's Information Risk Management towards 1000 organisations in United Kingdom and Ireland in 1998, they found that electronic commerce represents a major security threat where over three-quarters of the organizations using Internet had not tested the security of their Internet sites.

Through our survey we found that, organisations which involve in this line of business are highly dependent on computers in operating their business activities (figure 2). Logically, if we look at the finding, we can say that these organizations have great exposure to the threat of computer related crime because of the intensive use of computers in their business activities. Thompson (1998) found that there is a direct correlation between those industry groups that experienced the most intrusions, or other unauthorized use of computer systems and those that had the highest level of computer use in the workplace. More importantly, all of respondents reported that their computer systems are inter-networked whether corporate local area network, wide area network or global area networks (figure 3). Computer systems that are inter-networked are threatened not just from inside but from outside parties too. From our survey, we found that there are incidents where people outside the organisation commit the intrusions although less than people inside the organization do. Both intrusions can only be done by effective use of networking support. Garry Dinnie from Ernst & Young (1999) mentioned that network security is a continuing concern in his Second Annual Global Information Security Survey which canvassed the opinions of more than 4,254 companies in 29 countries around the world. In addition, he found that 78% of organizations are not confident about their network

safety from internal attack, while 50% lack confidence about their security against external attack.

Out of 35 respondents, only 8 respondents (22.86%) acknowledged that their systems had been broken into. If we conclude from the percentage, we can say that computer crime is not very critical yet in Malaysia compared to other countries likes United States, Britain and Australia. Survey done by Thompson (1998) found that 54% of the respondents have experienced unauthorized use of their computers in Australia. Moreover, there is an increase of security breaches in United States since 1996 to 1999 (42% to 62%) which was reported by Computer Security Institute. Perhaps, this increment is closely related to the wide use of computers in their countries compared to Malaysia. However, in our survey, we are not so sure with the response of respondents towards security breaches. There are two reasons, which need to be considered in discussing this finding. First, it is possible that the respondents are not aware that unauthorised persons have intruded into their systems. Second, may be respondents are not willing to disclose to the public that their companies had been broken into. According to McCune (1998), some companies do not report any intrusion into their systems because they may be unaware or too embarrassed to talk about it even if they are. In addition, he did give an example of what had been done by Defence Information Systems agency, the computer arm of the Department of Defence in 1995. This agency tried to hack into 18, 000 U.S. government systems where a stunning 88% of the attacks were successful and 95% of those break-ins went undetected. Furthermore, Cruz (1998) did mention in his article that, the worst thing about this crime is that it is not being reported. A bank or a credit union is unlikely to report that their system was broken into, for fear of losing customers' trust and besides that, sometimes a business is not aware that a high-tech crime has happened.

Of the 8 respondents who experienced intrusion by unauthorised persons, 5 were from inside and 3 from outside the organization. According to Thompson (1998), nearly 87% of those that experienced a computer related incident identified a source as internal and approximately 60% as external to the organization. The overlap in these figures is due to some industry groups having experienced both internal and external abuse. Such results were generally consistent with similar surveys conducted in Europe and the U.S. (CSI, 1997 & 1999; Carter and Katz, 1996; UN Commission on Crime and Criminal Justice, 1995). It means that the threats are commonly generated from inside the organization. CSI (1999) reported that unauthorized access by insiders rose for the third straight year; from 37% of respondents in 1996 to 57% in 1999. So, it was no wonder, from our survey, we found that respondents rated disgruntled employees as a number one source of the breaches. The next source is criminal (personal gain) and followed by independent hacker or info broker.

Certainly, the growing use of computers has exposed an organization's system towards intrusion. Beside that, the new way of managing an organization from centralized to decentralized network has made it more vulnerable. We have to realize that in the future, the hackers are not just from inside the organization but it can be from outside or somewhere else where we can not identify. Previous and recent research on this area shows that threat from outsiders is growing steadily (CSI, 1997 & 1999; Dinnie, 1999; Thompson, 1998). Dinnie (1999) in his survey found that, companies are generally more concerned about external than internal threats. Hackers (53%) and unauthorized users (49%) are rated a greater threat than current employees/authorized users (31%). According to CSI (1999), perhaps the most disturbing trend is the continued increase in attacks from outside the organization. Our research findings also show a consistent result with others where respondents rank hacking as the one issue most likely to impact on their organizations over the next five years.

From our study we found that most of attack or intrusion into system can be characterized as unauthorised access. By the way, respondents were also concerned about unauthorized copying of data/programs, manipulation or alteration of data/programs, damage to data/program. On the other hand, 75% of those who experienced break-ins had identified the pattern of type of information accessed. Additionally, financial systems/data was the most attacked information. Beside that, in this study, the respondents also acknowledged other types of information such as confidential corporate data, intellectual property and personnel information. Our finding is consistent with Thompson (1998), where in his study, he found that financial systems and confidential corporate data were the two most frequently attacked information types. The recent annual survey (1999) by CSI has identified several types of attack as critical. It rose dramatically from 1998 to 1999, for examples, denial of service attacks (32%), sabotage of data or network (19%) and financial fraud (14%).

There is no doubt that an organisation will suffer a direct or indirect cost or loss associated with the unauthorised use of system. We found that, financial organisations in our study did not seriously suffer financial losses in conjunction with computer crime. All 8 respondents claimed that this crime cost them not more than RM 10, 000. If we look at the cost that they suffered, we can conclude that computer crime is not a big issue yet for our country. Interestingly, the same thing happened to a survey done by Thompson (1998), 77% of respondents estimating the total direct or indirect cost of incidents at under $ 10, 000. He was not satisfied with the above finding. Consequently, he did a prompt follow-up study with selected respondents which identified that the IT managers of organisations were not necessarily in the best position to estimate the full cost of computer abuse. At last, he discovered the truth, for example, one bank which participated in the survey had estimated the total cost of computer misuse for the past twelve months at less than $ 10, 000. However, he found out from the compliance and fraud control officer at the bank, that a "figure in excess of $ 500, 000 would be more realistic". This could happen because of two factors. First, may be the IT manager is not the right person to answer this question. Second, may be the organisation cannot quantify the losses or costs involved. Hopefully, this phenomenon could be justified if we refer to previous and recent research by CSI (1999). In their recent research reported that financial losses due to computer security breaches mounted to over a $100, 000, 000. Although 51% of respondents acknowledged suffering financial losses, only 31% were able to quantify their losses. The most serious financial losses occurred through theft of proprietary information (23 respondents reported a total of $42, 496,000) and financial fraud (27 respondents reported a total of $39, 706, 000).

Information Securities Policies and Procedures

KPMG has defined information securities as "the practices and procedures which ensure that information, generally held in electronic format, is safeguarded from unauthorised access, modification or accidental change and is readily available to authorised users on request". Moreover, in introduction on managing security of information by International Federation of Accountants (IFAC), it stressed that in a digital world the effective management of information, information systems and communications is of critical importance to the success and survival of an organisation. This critically arises from the increasing dependence on information and the systems and communications that deliver the information, the scale and cost of the current and future investments in information and the potential for technologies to dramatically change organisations and business practices, create new opportunities and reduce costs. In addition,

Dinnie (1999) showed that information security risks have increased where a total of 57% of companies said their risks are higher now than a year ago and only 4 % said their risks have reduced. Executive management should take responsibilities instead of IT personnel in safeguarding the information (Dinnie, 1999; IFAC, 1998). So in order to fulfil the responsibility, an executive management should ensure that their organisation have in place proper and adequate security policies and procedures towards the system.

From our survey, we found that out of 30 respondents, 73.33% had performed a qualitative and/or quantitative risk assessment to determine the specific areas of potential risk that could impact their ability to perform day-to-day business functions. In addition, 67% of them answered that risk assessment had been prioritised to facilitate budget allocations. As discussed by many audit textbooks (Aren, (2000); Cosserat, (2000); Whittington, (1999)), before we can put effective and efficient control or security measures through out the systems, we need to know what are we going to control, why and the cost and benefit of the control activities. So, performing a risk assessment is very important because from that we can decide what level of risk is acceptable and give us a guidance on how to allocate resources that we have to ensure a uniform level of security across all key systems (Dinnie, 1999). However, it is useless if management does not see the importance of these issues and does not give priority to facilitate budget allocations towards these risks. Normally losses or costs of the damage are higher than cost of control activities. Interestingly, from our survey, we found that financial institutions are aware of information security risk in their business operations. This result is consistent with survey done by Thompson (1998), where in his research, three sectors stood out as meeting above criteria namely banking and finance, technology/communications/computing and government. On the other hand, Ginnie (1999) found that a total of 45 % of companies made no budget allowance for information security and 41% had no budget for business continuity program. There is a slightly different in result between Ginnie and ours and Thompson. This could be because of the respondents. We just concentrated on financial institutions in Malaysia, which is consistent with Thompson finding where only 3 sectors were identified meeting the criteria. While Dinnie's respondents come from across the world. Furthermore, we strongly believe that financial institutions are more concerned about security compared to other industries since they are favourite target of intruders (Thompson, (1998); Carter & Katz, (1996).

In the area of risk management, 83.9% organisations have a written policy on the security and misuse of computing facilities. Surprisingly Thompson (1998) reported that nearly 60% of respondents had no policy on how to deal with system breaches and 70% reported by CSI (1996). Furthermore, 69.2% of respondents from our survey claimed that their policy include sanction/procedures for dealing with breaches. However, only 42.3% of respondents acknowledged that their policy includes provisions for notifying appropriate law enforcement agency of breaches. Interestingly, Thompson (1998) also reported the same thing at about 73% and 50% by CSI (1996). In addition, 70% of the respondents had no policy or procedures for preserving evidence for civil or criminal proceedings after a security breach in which valuable information has been compromised. Thompson (1998) also reported a high percentage on this matter (70%). In this area, we can say that, financial institutions have taken appropriate security measures by their own but it seems like they do not have a good relation with law enforcement agency. Through our research, we found that only 13.04% of respondents will report an incident to a law enforcement agency. In contrast, approximately 47.83% of respondents will did their best to patch security holes of the system. Some of them will report to solicitor to seek civil remedy and external incident response team.

We found that 90% of respondents claimed that their organisations routinely conduct system security audits. And 86% maintained historical records or data of system misuse or intrusion attempts. System security log and audit log is the favourite place to maintain the records or data.

Our research results show that, financial institutions have taken serious steps to prevent and protect their system from intrusion by unauthorised persons. However, Thompson (1998) concludes that the Australian industry on the whole was poorly prepared in many areas. This becomes particularly evident when compared to similar survey conducted by CSI in 1996. Additionally, a survey done by Dinnie (1999) found that a total of 75% of senior managers rate information security as "important" or 'extremely important" but their concern is not reflected in organisational procedures where 30% of companies have no formal policies and procedures relating to information security.

Security Awareness

In auditing, control environment is one of the components in internal control system. Control environment will create an environment where people especially employees are aware that control and security are important and that they should follow a written policy and procedures in performing their tasks and duties. Once again, top management should play important roles in showing that control and security are important in the organisation.

In our study, we found that 73.3% of organisations have a computer security awareness program for all employees using information technology. In addition, 96.8% instruct their employees in the ethics of using computers and technology. However, only 21.2% of the employees with access to computer and telecommunications systems have a working knowledge of the current laws of misuse of computer systems. In the event of an incident, police rank as the first law enforcement agency to be contacted, followed by Bank Negara Malaysia, Security Commission, lawyers and MIMOS. They will contacted because of company policy (20.9%), prosecute offender (19.4%) and followed by making an insurance claim (11.94%). By the way, only 17.2% maintain liaison with law enforcement agencies regarding misuse or unauthorised access of computer systems. The main reasons for not maintaining liaison are incidents too infrequent, all action taken is of civil nature and followed by do not know whom to contact. 29.73% organisations willing to report computer related crime incidents to law enforcement if they got chance to recover the loss, 21.62% immediately when detected and followed by 18.92% if mandatory by law.

Conclusion and recommendations

In general, the results of this study showed that financial institutions in Malaysia are not seriously threatened by computer crime compared to United States, Europe and Australia. Moreover, they are also aware and have been taken several steps regarding securities policy and procedures of their systems. However, we should not feel comfortable and secure with the finding. It is because one of the problems with computer crime is that management for fear of losing credibility and exposing their weaknesses often does not report incidents.

From our point of view, this issue is a crucial element in our country development agenda if we are going to be an electronic country in the near future. We should realise that, the problem will

multiply as nowadays people are not just computer literate but also networks literate. And as explained earlier, the intruders could be from anywhere. An organisation whether profit or non-profit oriented should work together with law enforcement agencies to prevent and overcome this issue. They must develop policies, methods and regulations to detect incursions, investigate and prosecute the perpetrators and prevent future crimes. So far, we have Computer Crime Act (1997) but we are not sure yet how effective this act is when it comes to enforcement. From our survey, we found that financial institutions do not have good relations with law enforcement agencies.

There are lots of issues in computer crime that need to be studied for a better understanding of issues related to it. Research can be done probably on origins, methods and motivations of these growing criminal groups. Besides that, what action should be taken by law enforcement agencies to cope with this problem.

References:

Arens, A. A., Loebbecke, J.K. (2000), Auditing: an Integrated Approach, 8th ed., Prentice hall.

Arey, D., (1997), Tech Crime Still an Inside Job, Crain's Chicago Business, 1/27/97, Vol. 20 Issue 4, pp10-11.

Bort, J., (1997), Liar, Liar, Client Survey Computing, May 97, Vol.4 Issue 5, pp 40-43.

Carter, D.L. and Katz, A.J., (1996), Computer Crime and Security, Security Journal, No 7, pp 101-108.

Carter, D.L. and Katz, A. J., (1996), Computer Crime an Emerging Challenge for Law Enforcement, FBI Law Enforcement Bulletin, Dec 96, Vol. 65, Issue 12, pp 1-7.

Carter, D.L. and Katz, A.J., (1995), Computer Crime Categories, FBI Law Enforcement Bulletin, Jul 95, Vol. 64 Issue 7, pp 21-26.

Computer Security Institutes (CSI) (1998), Computer Crime and Security Survey, http://www.gocsi.com

Conley, J.M. and Bryan, R.M., (1999), A survey of Computer Crime Legislation in the United States, Information & Technology Law, Mar 99, Vol.8 Issue 1, pp 35-57.

Cosserat, G.W. and Gill, G. S., (2000), Modern Auditing in Australia, 5th Ed., John Wiley & Sons.

Cruz, S., (1998), Computer Crime Unreported, Undetected, Las Vegas Business Press, 04/27/98, Vol. 15 Issue 17, pp 3-4.

Davis, S.H., (1998), Internet Innocence Lost, Telephony, 03/30/98, Vol. 234 Issue 13, pp 5.

Dinnie, G., (1999), The Second Annual Global Information Security Survey, Information Management and Computer Security, Vol. 7 Issue 3, pp 112-120.

Doney, L.D., (1998), The Growing Threat of Computer Crime in Small Businesses, Business Horizons, May/Jun 98, Vol. 41 Issue 3, pp 81-86.

Elliott, R.S., (1996), Computer Crime Poses Growing Threat to Businesses, Inside Tuchson Business, 07/15/96, Vol. 6 Issue 16, pp 3-4.

Elmi, G.T., (1997), The Law on Computer Crime in Italy, Information & Communications Technology Law, Oct 97, Vol. 6 Issue 3, pp 249-265.

Friedman, M., (1998), It's Still Game Set and match for Those Annoying Spammers, Computing Canada, 10/19/98, Vol. 34 Issue 39, pp 6-9.

Information Security Survey 1998, http://www.kpmg.co.uk

International Federation of Accountants, (1998), Internal Information Technology Guideline

on Managing Security of Information, http://www.ifac.org.

Martin, E. (1997), High-tech Crime's hidden face, Business Journal Serving Charlotte & the Metropolitan Area, 10/13/97, Vol. 12 Issue 27, pp 25-27.

Matthew, K.O.Lee, (1995), Legal Control of Computer Crime in Hong Kong, Information Management & Computer Security, Vol. 3 No. 2, 1995, pp 13-19.

McCollum, T., (1997), Computer Crime, Nation's Business, Nov 97, Vol.85 Issue 11, pp 18-25.

McCune, J.C., (1998), How Safe Is Your Data, Management Review, Oct 98, Vol. 87 Issue 9, pp 17-21.

Moscove, S.A. and et.al., (1997), Core Concepts of Accounting Information Systems, John Wiley & Sons, Inc.

Multimedia Development Corporation, http://www.mdc.com.my

Pearsall, K., (1998), Companies Fear Publicity When Reporting Network Break-ins, Computer Dealer News, 04/20/98, Vol. 14 Issue 15, pp 43.

Romney, M.B. and et. al., (1997), Accounting Information System, Addison-Wesley Longman, Inc.

Rosenkrantz, H., (1996), Computer Crime Creates Growth Potential in Cyberspace, Fairfield County Business Journal, 10/21/96, Vol. 35 Issue 43, pp 5.

Roush, W. and McIntosh, J., (1995), Hackers: Taking a Byte Out of Computer Crime, Technology Review, Apr 95, Vol.98 Issue 3, pp 32-40.

Roufaiel, N.S., and Dorweiler, V., (1994), White-collar Computer Crimes: A Threat to Auditors and Organization, Managerial Auditing Journal, Vol. 9 No. 3, 1994, pp 3-12.

Schmidt, B., (1994), Computer Criminals Race Deterrents, Sacramento Business Journal, 3/14/94, Vol. 10 Issue 51, pp 15-16.

Speech by Louis J.Freeh, Director of the FBI, 1997 International Computer Crime Conference, New York, March 4, 1997, http://www.fbi.gov

The Kuala Lumpur Bankers Directory 1998/99, Arab-Malaysian Merchant Bank Berhad.

Thompson, D., (1998), 1997 Computer Crime and Security Survey, Information Management & Computer Security, Vol. 6 Issue 2, pp78-101.

UN Commission on Crime and Criminal Justice (1995), Manual on the Prevention and Control of Computer-related Crime, New York, NY, 1995.

Welch, T., (1997), Computer Crime Investigation and Computer Forensics, Information Systems Security, Summer97, Vol. 6 Issue 2, pp 56-80.

United States, Department of Justice, http://www.doj.gov

Whittington, O.R. and Pany, K. (1998), Principles of Auditing, 12th Ed., mcGraw-Hill.

Appendix

Table 3

Risk Assessment and Risk Management

QuestionsAsked	Respondent %	Yes %	no %	don't know %
Has you organisation performed a qualitative and quantitative assessment?	30	73.33	20	6.67
Have risk assessment results been priotitized to fasilitate budget allocation?	27	67	25.9	7.1
Written policy on the security and misus of computing facilities?	31	83.9	12.9	
Written policy include how to deal with network intrusions?	26	69.2	30.8	3.2
Written policy include sanctions/procedures for dealing with breaches?	27	67	30	3
Written policy include provisions for notifying appropriate law enforcement authorities of breaches?	26	42.3	46	11.7
Does your organisation have any policy/procedures for preserving evidence for civil or criminal proceedings after a security breach in which valuable information has been compromised?	30	30	63	7
Does your organisation have a computer security awareness programs for all employeess using information technology?	30	73.3	23.3	3.4
Does your organisation instruct its employees in the ethis of using computer and technology?	32	96.8	0	3.2
Do employees with access to computer and telecommunications systems have a working knowledge of th current laws on misuse of computer systems?	33	21.2(most)	72.79(few)	6.1(none)