Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 1995 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

December 1995

On Computer Security Issues in Hong Kong

Hakman Wan
Lingnan College

On Computer Security Issues in Hong Kong*

Hakman A. Wan
Department of Computer Studies
Lingnan College, Hong Kong

Abstract

This paper describes how the Computer Crime Ordinance is implemented in Hong Kong. It identifies a few weaknesses in the laws and suggests some security measures to defend information systems in Hong Kong against possible exploitation by perpetrators. Two court cases are reported and they may be informative to the profession of information system security.

1 Introduction

After a long consultation period, the Hong Kong Government finally gazetted its Computer Crimes Bill in March, 1992. The Bill was converted to laws a year later and since then, the computer profession is supposed to be protected by these laws.

Computer service are mostly targeted towards small- to medium-sized businesses; though many of them are satisfied with simple PC applications, many others invest generously in their information systems. According to a 1992 survey [Kamay 92], these organizations are equipped with hardware and software whose values amount to HK$4 million on average. Some of them have more expensive installations which are worth over HK$80 million.

Not alone in the world, many organizations in Hong Kong have experienced a variety of computer abuses and suffered from various degrees of risks in their information systems [Kamay 92]. There is a general understanding that most business organizations are reluctant to report cases of computer abuses, even if they were found out. Considerations believed to be strong reasons behind these unreported crimes [Chantico 92] include:

- fear of adverse publicity,
- fear of lawsuits by persons whose records have been exposed,
- fear of opening up the company to further attacks, and
- fear of charges that their computer systems are not secure.

*The author would like to thank Mr. Wanbil Lee, Head of the Department of Computer Studies, Lingnan College and the anonymous reviewer of this conference, for their kind support and valuable comments on the writing of this paper.

Therefore, it is estimated that, in US, less than 25% of all so-called white-collar crimes are ever reported. Hong Kong businesses have the same worries. Any such cases made public are believed to represent only the tip of an iceberg. If computer crimes are going to be encouraged by hi-tech on one hand and unsuccessful attempts in prosecution on the other, business information systems in the district will become more and more vulnerable. The loss will be astronomical. According to the Commercial Crime Bureau of Hong Kong [SCMP Post 6/2/95], a reported case suffered a loss of $500,000. Considering the size of business in Hong Kong today, a spokesman of the Bureau would not be surprised if a loss of business deals of $100 million is reported.

This paper aims to pinpoint the inadequacies of the legislation. The story of computer crime legislation is described in the next section. Their weaknesses, mentioned in Section 3, may put computer perpetrators in a better position to excuse themselves from being charged. In Section 4, some suggestions are made to re-enforce the defense line. A conclusion ends the paper in Section 5.

2 The Computer Crime Ordinance in Hong Kong

The Computer Crime Ordinance is not introduced as a new *sui generis* legislation in Hong Kong. By amending the existing criminal codes relating to telecommunications, computer crimes, theft, fraud and abuse are included as criminal offenses [Lee 94]. This is an efficient way of legislation and is a common practice among most English-speaking countries and many European countries [Sieber 86].

'Unauthorized access' seems to be universally accepted as the first thing that an information system has to guard against. Thus, as stated in Section 27A of the Telecommunication Ordinance,

> Any person who, by telecommunication, knowingly causes a computer to perform any function to obtain unauthorized access to program or data held in a computer commits an offense and is liable on conviction to a fine of $20,000.

The term 'telecommunication' here takes a generalized meaning which includes the usage of all means of electromagnetic devices, for example, a telephone network. As

pointed out by [Davies 92] and [Lee 94], such statement does not require the defendant to succeed in obtaining access to the programs or data. Any attempt, even as simple as merely causing the computer's security device to be activated, is sufficient to constitute 'an unauthorized access.'

However, [Lee 94] adds that using voice input to activate a computer falls outside the scope of telecommunication. The argument is 'human voice communication is based on sound pressure waves and not electromagnetic principle.' To the author of this paper, it could be a subject for debate. There should be a different view: even human voice communication is triggered by vibrations of a person's vocal cord, the audio receiving device at the other end (ie, the computer capable of listening to the input) must have some means to convert acoustic waves to electromagnetic waves. The law-maker obviously does not see this as a weakness; and the expansion of the meaning of 'telecommunication means' is natural if the law is put under the Telecommunication Ordinance.

Or, perhaps in a later day, the definition of 'Unauthorized use of computer' could be revised to a less controversial statement, for example, as the Section 301.2 of the Criminal Law Amendment Act 1985 of the Canadian Criminal Code [Tantam 91]:

> Every one who, fraudulently and without colour of right, ... by means of an electromagnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system.

If attempts to keep away unauthorized access to an information system fail, the perpetrators may tamper with valuable assets in the system: programs, data, and etc. These assets are properties of their lawful proprietors. Any attempt in manipulating these properties constitutes a criminal offense. It is not surprising to see two amendments in the Crime Ordinance, as pointed out by [Lee 94], in the definition of 'property':

(a) The term "property" now specifically includes any computer program or data held in any form and by any medium.

(b) Property damage now includes:
   (1) causing a computer not to function normally;
   (2) altering or erasing any program or data held in any form and by any medium;
   (3) adding any program or data to the contents of a computer or any computer storage medium.

Such definition provides the law people a strong weapon to scare away any person with an intent to destroy, erase, or alter data stored in or to insert data into a computer; certainly it is also targeted at anyone who tries to infect a computer with viruses. But furthermore, according to [Lee 94], the offense is constituted once the evidence of unauthorized tampering with the information system is proved, no matter whether the information system is impaired.

The act of burglary has also been taken care of. The definition of 'Property damage' is repeated in the Theft Ordinance. Now the offence of burglary includes [Lee 94] physical trespassing in a building with the intention of

(1) causing a computer not to function normally;
(2) altering or erasing any program or data held in any form and by any medium;
(3) adding any program or data to the contents of a computer or any computer storage medium.

Nobody really knows exactly how effective these laws could be. When the Ordinances were first introduced, the Hong Kong Government had promised a review after 12 months [SCMP Post 2/6/95]. However, with a small number of reported cases (only 12 up to Feb 6, 95 [SCMP Post 2/6/95]), law-enforcement experts may not be able to discover niche or to gather sufficient evidence to support any amendment claim in the laws.

3 Difficulties in Prosecution

The evidence of 'lack of authorization' is generally the most difficult subject in proving a computer crime. Contrary to general speculations, many of the criminals are company employees. Fraud is very often committed by people in relatively trusted positions [Kamay 92]. When 'authorization' can be regarded as a formality, any proof of 'unauthorized tampering' becomes insignificant.

It could be easier if the employees are each clearly informed of their level of privilege in a policy document. But this is not normal practice. Furthermore, under the *mens rea* principle, the criminal intent of an action must be proved, ie, that the culprit was aware at the time that he/she was exceeding his/her authorization [Tantam 91].

Tampering with computers, programs, or data can also be protected by the necessity of *mens rea*. As pointed out in [Lee 94], an accused is not guilty if he/she can prove on a balance of probability that at the time of the alleged commission of the offence:

1. he/she believed he/she had been given consent by the person(s) entitled to give such consent to do any of the activities alleged; or
2. he/she believed he/she would have been given consent by the person(s) entitled to give such consent if the person knew all the relevant circumstances.

The spirit of *mens rea* protects an accused who genuinely believes in so, no matter whether or not the belief is reasonable.

It is, thus, not easy to bring computer criminals to justice. Evidence collection and preservation in the site of computer crime is different from crimes of other nature. Without proper training, investigators may easily overlook or even destroy important clues. Today, the Commercial Crime Bureau of Hong Kong is determined to fight against computer abuses. To train its personnel to cope with the advancement of computer criminals, the Bureau seeks help from FBI of USA [SCMP Post 6/2/95].

4 Security Measures

Among all kinds of computer security measures, the vulnerability of a security system depends on human values [Bloombecker 92]. It depends on how successfully senior management and other users are convinced of the importance of protecting information. It is difficult to have a security system keeping in pace with the rapid technological change, particularly in networking area. The protection of valuable strategic information requires something more than just legislation or technical responses.

Access control is the first and the most important defense of the computer system. The physical control, perhaps sounds less significant in other countries, is particularly important in Hong Kong environment. Since networking is not as popular as in other countries, computer systems in many large local organizations are not accessible from outside the premises that house the computers. The logical control by *identification* and *authentication* is the most popular and effective method. When a user is identified and authenticated, he/she is authorized to access the computer system in a pre-defined level.

Many organizations rely on their EDP auditors to discover computer frauds. This also becomes one of the reasons to consider security measures at the design stage of the system. In order to detect unusual activities, EDP auditors must lay various kinds of controls in the information system [Lee 89]. To identify critical paths of possible intrusions and to solve technical problems that may arise, the computer professionals must work side by side with the auditors to plant effective controls in optimal locations.

A general procedure is to keep an activity log of every user in an inaccessible place. Besides the second point mentioned above, a computer log may not be the most efficient way to work with. Since the volume of such log files expands in an astonishingly high rate, an unusual pattern of activities can hardly be recognized without the use of some pattern recognition techniques and devices.

Last year, an senior immigration assistant in the Hong Kong Immigration Department was caught and pleaded guilty of unauthorized access to files of immigration stop list [SCMP Post 11/12/94]. The prosecution was successful only because the computer had kept a log of activities of every user.

Security forces internal and external to the organization should sometimes work together. In Hong Kong, a hacker was brought to court and was convicted [SCMP Post 4/29/95] by the successful collaboration between the security managers of *Supernet* and the Commercial Crime Bureau of the Royal Hong Kong Police. This is so far the first conviction under the Telecommunication Ordinance, Section 27A.

5 Conclusion

Hi-tech is a double-edged sword. With one edge, it can be used as a strategic tool for the organization. But the other blade, if not coped with equally hi-tech security measures, may bring painful experience to the organization. A large proportion of organizations is still relying on employee integrity as their only defense line against computer crimes [Bloombecker 92]. But both the popularity and the omnipotence of morality education in Computer Ethics are questionable. Without proper countermeasures, information systems are vulnerable to all kinds of computer crimes. Even legislation cannot scare away criminals and hackers. A thorough consideration of security strategy must be incorporated to the design and planning of the information system early in its development stage.

References

Bloombecker, B., Computer Ethics for Cynics, *Computer World*, February 29, 1988, p.17.

Chantico, *Combating Computer Crime: prevention, detection, investigation*, McGraw-Hill, 1992, p.12.

Davies, J.R., Computer-aided Fraud and the Law, *Management Accounting*, October, 1992, pp.36-38.

Kamay, V. *et. al*, *Computer Security in Hong Kong*, Reprographic Unit, Hong Kong Polytechnic, July, 1992.

Lee, M.K.O., Legal Aspects of Computer Crimes and Information Systems in Hong Kong, *Working Papers Series* WP94/04, City Polytechnic of Hong Kong, January 1994.

Lee, W.W., Automation of Internal Control Evaluation, Caelli, W.J. (Ed.) *Computer Security in the Age of Information*, Elsevier, 1989.

Sieber, U., *The International Handbook on Computer Crime*, Wiley, 1986.

South China Morning Post, FBI help sought to trap hackers, Feb 2, 1995.

South China Morning Post, Hacker faces $45,000 bill, April 29, 1995.

South China Morning Post, Official guilty of running check on stop list, Nov 12, 1994.

Tantam, M., *Computer Abuse Investigator*, Elsevier Science Publishers Ltd, 1991.