EFFECTIVE COUNTERMEASURES AGAINST ECONOMIC CRIME AND COMPUTER CRIME

*Soh Thiam Sim**

I. INTRODUCTION

In the last two decades, the Asia-Pacific region has made significant economic progress. Economic growth has led to an increase in the region's wealth and purchasing power. Money, people and goods can move with greater ease from one state to another. However, such developments have opened up opportunities for cross-border economic criminals to thrive. Due to its increased wealth, the Asia Pacific region has inevitably become a target of economic crime. Singapore is also not spared and commercial crime has resulted in a total loss of about S$78 million in 1997.

Apart from increased wealth, the advent of information technology in the Asia Pacific has made communications and business transactions more sophisticated. As the region enters the information age, the use of computers in both commercial and non-commercial environment has increased significantly. While information technology enables business enterprises to compete globally and provides for a higher quality of life, it also enables criminals to commit a whole range of computer and computer-related crime. Indeed, the FBI predicted that in the near future almost every major crime would involve the use of some form of information technology. The emergence of new and complex techno-crime and the cross-border nature of syndicated economic crime have posed problems to the law enforcement agencies. The challenge to the law enforcement agencies lies in devising effective measures to counter such crime.

Economic crime can range from fraud, embezzlement, forgery, insurance fraud, and computer-related offences to insider trading, and organised crime schemes involving money laundering. In Singapore, the agencies investigating economic crime are the police and the Commercial Affairs Department (CAD) which comes under the Ministry of Finance. Most of the commercial crime cases are investigated by the police in the Police Land Divisions while the complex cases are investigated by the Commercial Crime Division (CCD) of the Criminal Investigation Department. The cases handled by the CAD are more specialised, eg offences under the Companies Act, the Banking Act, the Securities Industry Act and fraud and embezzlement involving company officials who abuse their position of trust. On the other hand, computer crime cases are investigated by the Computer Crime Branch which is one of the four branches under the CCD.

The following four specific types of commercial crime and computer crime continue to be areas of concern as Singapore strives to be a financial/ transport center and IT hub in the region:

(i) counterfeit credit card fraud;
(ii) maritime fraud;
(iii) documents of identity fraud; and
(iv) advance fee and telegraphic transfer fraud.

This paper was prepared to share with

* Head, Computer Crime Branch, Commercial Crime Division, Criminal Investigation Department, Singapore Police Force, Singapore

you some of our experience in handling these types of crime and the countermeasures adopted. The material for this paper is based largely on the experience of CCD.

II. CREDIT CARD FRAUD

A. Background

Unlike cash, credit cards operate in an international payment system, crossing jurisdictional confines. A credit card transaction can be made anywhere in the world. Currently, there are more than 700 million credit cards in circulation globally. Nearly 22,000 financial institutions are issuers of credit cards. About 13 million merchants world-wide accept cards as payment. The total annual cardholders' spending exceed US$1 Trillion. Credit cards have thus become a lucrative business and an integral part of the banking world. Its use has gained overwhelming popularity in the Asia Pacific region in recent years, including in Singapore.

The increase in card usage has led to a rise in card fraud. In 1996, the industry lost US$2.1 billion globally to card fraud, double that of 1995. Credit card fraud is committed by both petty offenders operating on their own and by well organised syndicates. From arrests handled by the Singapore Police, it appears that syndicates have built themselves a network between Malaysia, Thailand, Singapore, Indonesia, Hong Kong, Japan, Europe, South Africa and the U.K.

B. Types of Credit Card Fraud

Credit card fraud is perpetrated in the following ways:

(i) *Lost & Stolen Cards:* When a card is misplaced, lost or stolen from the cardholder, the culprits use these cards to make purchases in the shortest possible time, before the cardholder is alerted. The only hurdle for the culprits is imitating the cardholder's signature and they are able to overcome it by producing a signature close to the cardholder's;

(ii) *Intercepted Cards:* Cards may be intercepted through the mail or by the internal staff before the cardholder receives it. As the newly issued card is unsigned, the culprit would append a signature before using it;

(iii) *Fraudulent Applications:* The culprits would apply for cards using a fictitious identity or the identity of another person. Upon receipt of the card, they would go on a shopping spree with no intention of making payment;

(iv) *Colluded Merchant Fraud:* Merchant fraud is multi-faceted. It can involve a dishonest merchant making multiple charges on an unsuspecting customer's card and submitting the fraudulent charge slips to the bank for payment. The merchant may also collude with other perpetrators to accept counterfeit cards for payment. A merchant may also steal a cardholder's card information and sell it to syndicates to make counterfeit cards;

(v) *Mail Order/Telephone Order (MOTO):* Dishonest cashiers or counter staff at shops may compromise a cardholder's account. Using computer software such as 'CreditMaster', valid card account numbers are generated from the shoppers' data. The culprits then order goods and services via telephone or mail, quoting the card account numbers and expiry dates. In such cases, the delivery addresses given by the culprits are usually vacant premises, or premises rented for the specific purpose of collecting the delivered goods;

(vi) *Altered Cards:* The culprits would alter the details on a genuine card which was stolen, lost or expired. Alteration is done through a 'heat process' whereby the account details on the face of the card are flattened and new account details are re-embossed and re-encoded. The genuine account holder would be unaware of this until they receive the statement of accounts showing the unauthorised transactions;

(vii) *White Plastic:* White Plastic is a blank plastic card, with an integrated magnetic stripe, that is used to imitate the functions of a credit card. It is not necessarily white in colour and does not bear any resemblance to a normal credit card. The culprits would emboss details of legitimate accounts on the plastic, or encode account details onto the magnetic strip, or both. As white plastic does not have the physical appearance of credit cards, they are often used with the connivance of dishonest merchants; and

(viii) *Counterfeit Cards:* Statistics show that organised syndicates using counterfeit cards perpetrate most credit card fraud. Advanced technology enables syndicates to produce counterfeit cards of close-to-genuine quality. The final stage of counterfeit card production is the encoding of genuine account details onto the cards. Such details are usually supplied by dishonest merchants who steal the information from cardholders.

C. Skimming Fraud- Latest Modus Operandi in Counterfeit Cards

By 1995, credit card fraud syndicates were able to penetrate the security systems of credit card companies and produce counterfeit cards complete with information and security codes using a "Skimmer Machine". In January 1995, credit card issuing banks in Singapore received complaints that their customers' cards had been used extensively in Europe. None of the cardholders, however, had lost their cards. Investigations conducted by CCD revealed that all the cards had been used at a local Karaoke lounge between May and October 1994. The information on the cards was stolen at the lounge and supplied to the syndicate to produce counterfeit cards. About 500 fraudulent transactions were made in Europe on these counterfeit cards, amounting to S$160,000.

The counterfeit cards were believed to have been produced with genuine cards' information which was captured by a portable card reader called a "skimmer". The skimmer can electronically record access codes encoded in the magnetic strip of the cards. Skimming fraud has hit the card industry world-wide, causing millions of dollars in losses. In recent years, the Asia Pacific region alone suffered losses from skimming exceeding US$10 million. More than 40 % of these losses were incurred in Japan. The detection of skimming activities is difficult as the Point of Compromise (POC) is very mobile.

In March 1998, CCD arrested a Malaysian for skimming fraud. The culprit, a waiter in a KTV lounge, had used the KTV lounge as a point of compromise

(POC) for skimming. He had obtained a skimming machine from another Malaysian and was promised M$50 for the details of each gold credit card he swiped. The culprit stole customers' card data by swiping the cards through his skimmer and furnished the information to the accomplice in Malaysia. Subsequently, counterfeit cards were made from the data captured in the skimmer and fraudulent charges amounting to S$16,260 incurred in Malaysia. The culprit was charged in Singapore in July 1998 for fraud offences. The Prosecution pressed for a deterrent sentence and he was sentenced to 5 years imprisonment.

D. Countermeasures

Given the nature of the crime, countermeasures against credit card fraud should be organised on a regional or international basis. The Singapore Police Force has thus undertaken the following:

(a) Intensify the sharing of information through regular meetings and exchanges with the card industry and international law enforcement agencies to cripple cross-border syndicates;

(b) Increase regional co-operation in ASEAN through:

  (i) Intelligence sharing. By setting up a database on such fraud reported in the ASEAN region, early detection and apprehension of criminals can be facilitated; and

  (ii) Appointing a liaison officer in each member country. This would help co-ordinate cross-border enquiries, investigations and exchange of information.

International co-operation should lead to development of effective strategies aimed at breaking up and defeating the spread of criminal organisations, including dismantling their alliances and support networks. To this end, legislative mechanisms could further international co-operation; legislation on asset seizure is one such means.

In the area of prevention, the card industry and law enforcement agencies feel that both merchants and cardholders play important roles in curtailing such fraud. Merchants must be accountable for the fraud that takes place at their outlets and cardholders should assist by providing information on suspicious transactions. However, these are short and medium term solutions. A long term solution would be to make cards more difficult to be duplicated.

In particular, for skimming fraud, there is presently no one standard preventive solution. Various Task Forces have been set up to devise strategies to combat skimming fraud. The card industry and law enforcement agencies agree that timely identification at the point of compromise (POC) sites and sharing of such information can contribute to the successful crackdown on such syndicates and thus a reduction of fraud losses. The Singapore Police also believes in training to strengthen officers' capabilities and upgrade their investigative skills through training on handling transnational economic crime. We would also press for deterrent sentences against criminals so as to prevent like-minded persons from committing crimes of a similar nature.

III. MARITIME FRAUD

A. Types of Maritime Fraud

Maritime fraud can range from the crude to the very sophisticated, from ship scuttling to stealing cargoes using 'phantom ships'. In most cases, it involves the issue of false or altered documents which misrepresent the existence of certain goods, their quality, value, ownership or location. The extent and complexity of such crimes may be beyond the capacity and jurisdiction of any single law enforcement agency to deal with. A law enforcement agency investigating such activities within its own country may not detect any particular criminal offence. However, when examined in totality, such activities may constitute a criminal conspiracy to commit fraud. However, the complications of jurisdictional boundaries make it difficult to apprehend and prosecute the offenders with success. Three common types of maritime fraud are:

(i) *Charter Party Fraud*: In charter-party fraud, the perpetrator would first charter a vessel from an unsuspecting ship owner. After paying the ship owner the initial instalment of the freight, the culprit would offer all the available cargo space to unwary shippers. When the second or subsequent payment is due to the ship owner, the culprit would abscond with all the freight charges that he has collected, rendering the ship owner incapable of delivering the cargo to its final destination. If the shippers or consignees refuse to pay any freight surcharge to complete the shipment, the ship owner is left with no alternative but to discharge the cargo at any port and sell it so as to recover the freight charges due;

(ii)*Ship Scuttling*: In ship scuttling, the perpetrator would charter or own an old vessel, and offer cargo space to unwary shippers at extremely low freight rates. Once the vessel is loaded with cargo, worth much more than the value of the vessel, it would set sail for an unscheduled port where the cargo is discharged and sold for the highest proceeds. The vessel would thereafter leave port for the high seas and be deliberately sunk. Having done this, the perpetrator would claim insurance not only for the lost vessel, but also for the full value of its cargo, purportedly lost together with the vessel; and

(iii)*Phantom Ships*: In recent years, phantom ship fraud has seen a significant increase in number. It is a developing phenomenon that requires close scrutiny. A 'phantom ship' is a vessel with a phantom identity. The registration of such a vessel is based on false information and documents provided by the perpetrators to the registering authority, and may include the vessel's name, owner's particulars and technical specifications. Such fraud is facilitated by ship registry officials who are not stringent and are prepared to grant provisional registration based on the unverified information and documents provided. Owners of phantom ships are usually shell companies using the premises of secretarial service providers, sometimes set up a few days prior to the illegal operation. The crew hired for the job are often of mixed nationalities and sometimes given false identities, thus making it extremely difficult to trace them when the phantom ship and its cargo 'disappear' in the high seas.

Between April 1997 and March 1998, CCD investigated three cases involving phantom ships. In two of the cases, Singapore companies had chartered the vessels for the carriage of cargo which subsequently disappeared en-route to the port of discharge. In the third case, the provisional voyage documents had been collected in Singapore. However, the Maritime and Port Authority records showed that none of the vessels had called at Singapore. Investigation conducted by

CCD however does not reveal any evidence to substantiate a criminal charge against any of the parties.

B. Countermeasures

As the investigation and prosecution of maritime fraud is fraught with problems of jurisdiction, the best approach is to work towards preventing it. Based on CCD's experience, some possible preventive measures include:

(i) Tightening procedures for the registration of marine vessels to prevent registration through the use of false or forged documents;

(ii) Installation of technologically advanced gadgets on board marine vessels, such as black boxes, to enhance the identifying and tracing of movements of vessels; and

(iii) Working in partnership with the shipping, freight and insurance industries, as well as with other law enforcement agencies.

IV. DOCUMENTS OF IDENTITY FRAUD

A. Background

The enhanced movement of people across borders has given rise to the use of fraudulent documents of identity. Fraudulent identification documents are used by illegal aliens to enter a country. Criminals also use fraudulent identification documents to prevent detection from law enforcement authorities. The use of fraudulent documents would make it laborious for law enforcers to establish a criminal's identity.

Whilst advanced technology has facilitated the production of high-quality identification documents, with improved anti-counterfeiting features, fraudsters have been able to match this by producing convincing fakes. Indeed, technology will continue to facilitate such fraud and pose challenges to law enforcement.

B. Types of Fraudulent Documents of Identity

In Singapore, four main types of fraudulent documents of identity have surfaced in recent years. They are:

(i) *Photo Substituted Passports*: where the genuine passport is either purchased or stolen from the owner. The syndicates would tamper with the passport's laminate and security features to change the photograph on it. Biological data may also be altered in the photo-substituted passport;

(ii) *Altered Passports*: which are often used by syndicate runners to smuggle children. A common ploy is to imprint a child's photograph with forged immigration endorsement onto a runner's passport. Fictitious biographical data may also be imprinted on the passport. An altered passport enables the runner to pass off as a guardian or parent of the smuggled child. Syndicates have attempted to smuggle Sri Lankan children using altered passports;

(iii) *Counterfeit Passports*: which are the least common of fraudulent passports. The distinguishing features in a counterfeit passport are the inferior quality and lack of security features. Counterfeit Singapore international passports were detected in the mid 1990s. However, this is a dwindling trend due to improved anti-counterfeiting security features in genuine passports; and

(iv) *Counterfeit Identity Cards*: Counterfeit Singapore identity cards were recently detected. The distinguishing features in a counterfeit identity card are the lack of security features and inferior quality. Most of the counterfeit identity cards had been used by illegal immigrants and illegal overstayers who tried to make their stay in Singapore appear legal.

C. Proliferation of Syndicates

Syndicates have grown significantly in recent years because of two main reasons. The first is the constant demand for such fraudulent documents. Fraudulent passports are in high demand as they are needed for illegal migration purposes. This demand is created when people want to migrate and look for jobs in other countries, but could not meet immigration requirements. The Singapore passport, particularly, is highly sought after for illegal entry purposes. The Singapore passport is popular because Singapore's multi-racial community enables illegals from various nationalities to pass off as Singaporeans in other countries. Its high demand has resulted in the emergence of fraudulent passport cross-border syndicates made up of Singaporeans, Chinese or Indians.

The second reason for the proliferation of such syndicates is profitability. Trafficking in fraudulent documents of identity has become a profitable venture. Alien smuggling rackets, for instance, may charge between S$6,000 and S$12,000 for a 'package' which could include a fraudulent passport, accommodation and air ticket. During an operation in June 1996, police arrested 20 Chinese nationals who attempted to leave Singapore with fraudulent Singapore international passports. If we assume the subjects were charged S$6,000 each, this particular venture would have generated S$120,000 for the syndicate.

D. Countermeasures

Document fraud, in particular involving criminal syndicates, may be tackled from 4 broad angles:

(i) *Prevention*: A preventive strategy may be adopted to counter such fraud. For instance, the document of identity may be made tamper-proof and forgery-proof. In the case of Singapore passports, much of the abuse occurs in other countries. Presently, the Singapore international passport is being re-designed. Features deterring photo-substitution, counterfeit and forgery have been factored into the passport's new design and make. The re-design process is still in progress. Other countries could similarly review their passport design to prevent document fraud.

(ii) *Detection*: Another vital strategy is detection. This may be facilitated by a good intelligence network which can ferret out the criminals. Currently, information on criminals involved in such activities is scarce. End-users of these fraudulent documents are often reluctant to cooperate with law enforcers. Intelligence is often the key to detection. For instance, the intelligence and investigation initiatives of the Singapore Police have resulted in the prosecution of several alien smuggling syndicates. Between 1995 and 1997, 465 persons of various nationalities were identified and prosecuted in Singapore for passport-related offences. These persons included both syndicate leaders and runners, as well as users of the fraudulent passports;

(iii) *Deterrence*: In Singapore, the authorities take a stern view of fraudulent passport offences. Courts are urged to impose deterrent sentences on those convicted of such activities. Those convicted of selling their passports are also denied future passport facilities. These measures help deter fraudulent passport syndicates and quell the supply of Singapore passports to illegal aliens; and

(iv) *International Co-operation*: Close cooperation on a regional and international basis, is another key strategy which could be adopted. Law enforcement agencies could work closely and pinpoint transit points and sources of illegal aliens. Singapore participates in ASEAN-organised discussions on trends in alien smuggling and coordinated efforts in combating the problem. Regional states could also work closely through existing Interpol channels to combat these problems.

Accelerated enforcement pressure will cause criminals to change tactics. Also, with access to the latest technology, it is unlikely that fraudulent identity document syndicates can be easily eradicated. In fact, documents of identity fraud will become more sophisticated. Law enforcement agencies may also have to employ new measures and seek new alliances, eg working closely with the airline industry, in order to identify emerging trends and nip these developments in the bud.

V. ADVANCED FEE & TELEGRAPHIC TRANSFER FRAUD

A. Advanced Fee Fraud - Nigerian Scams

In recent years, African nationals, operating alone or as part of larger syndicates, have employed several methods to perpetrate large scale and elaborate scams in this region. One such target is Singapore, perhaps because of its reputation as a business and financial centre. Such scams often involve extracting an advance fee from victims to transfer non-existent overseas funds.

In the early 1990s, such fraud was perpetrated largely by syndicates in Nigeria. There are several variations in the modus operandi of Nigerian scams. The following are the two more common scams:

(i) *Bank Deposit Scams*: A syndicate member claiming to be a high-ranking government official, would send letters to various recipients, mostly businessmen. The victims are invited to receive transfers of large sums of money into their bank accounts in return for a commission. The syndicate would claim that the money is excess government funds left from over-invoiced government projects. The victims are advised to send them their bank account particulars, company letterheads and pre-signed company invoices, and also lured to Africa to purportedly arrange for the funds. Once the offer is accepted, the syndicates make the recipients pay various forms of advance fees, ostensibly for administrative purposes such as local taxes, legal fees, money-transfer fees and bribery. In Singapore, local companies and individuals in Singapore have been forwarding

Nigerian letters to CCD. In 1995, a total of 551 letters was received but this decreased to 414 in 1996 and 187 in 1997; and

(ii) *Money Duplicating Scams*: Another modus operandi commonly applied is the 'money duplicating scams'. Syndicates lure victims into believing that US dollar notes may be duplicated after treatment by 'special chemicals'. Victims are shown demonstrations during which currency notes are duplicated. The culprits then cheat their victims into making advance payments ostensibly to purchase the 'special chemicals'.

The increasing number of such scams has prompted Interpol's Secretary General to label them as "advance-fee frauds". He has also issued a general alert to all member countries. African advance fee fraud, like other economic crime, is subject to changes in technology. With hi-tech channels replacing conventional modes of commercial transactions, criminals now have a wider, global reach. The Internet for example is increasingly being used as a communication means. Its relative low cost has facilitated the entry of new players and providers. Its usefulness, however, is frequently abused by criminal enterprises. It is therefore not surprising that African advance fee fraud is increasingly perpetuated via the Internet. Again, law enforcement agencies would have to find updated means to combat these new problems.

B. Telegraphic Transfer Fraud

Recent cases investigated by Singapore's CCD indicate that syndicates emanating from Africa were engaged in telegraphic transfer fraud. In these cases, banks in Britain and the USA received letters purportedly from their account holders, authorising the wire transfer of money to the culprits at Singapore banks. Between March and April 1998, CCD handled 3 such cases. The sums involved ranged from US$10,000 to US$40,000. However, the African culprits were not able to withdraw the money successfully when they called at the Singapore banks. This was because the local authorities were alerted in time by the UK and US enforcement agencies. The close working relationship between the banks and CCD resulted in the arrest of the African culprits. They were charged in court for offences of attempted cheating and possession of forged documents and sentenced to imprisonment terms ranging from 12 to 24 months.

Like many types of cross-border crime, telegraphic transfer fraud confronts the problem of comprehensive solvability. In telegraphic transfer fraud, a fraudulent release of money in one country would result in the illegal receipt of money in another country. Even though the offender is successfully prosecuted in one country, the law enforcement agency would have solved only a part of the crime. Jurisdictional limits often hamper such crime from being solved as a whole.

C. Countermeasures

Advance fee fraud and telegraphic transfer fraud may be tackled using the following broad strategies:

(i) *Prevention*: Public awareness of such scams is a key preventive strategy. The Singapore Police works with the local media to increase Singaporeans' awareness of such scams. As such scams may come on and off, the public should be alerted on a periodic basis. This has proven to be a successful strategy as the number of victims cheated have declined over the years;

(ii) *Detection*: As with most cross-border crime, detection through a good intelligence network is another useful strategy. Currently, victims often hesitate to report the crimes for fear of embarrassment. There is thus little information for law enforcers to work on. In Singapore, Police-initiated intelligence efforts have resulted in the detection of several African nationals involved in advanced fee fraud. Between 1995 and 1998, 7 different syndicates were uncovered and prosecuted for criminal offences;

(iii) *Deterrence*: In Singapore, courts are often urged to impose deterrent sentences on those convicted of fraudulent advance fee activities. The tough penalties could serve to deter such fraudsters from making Singapore a target of such scams; and

(iv) *Enforcement*: In view of the cross-border nature of advance fee and telegraphic transfer fraud, law enforcement agencies should work closely with one another to fight such crime. This would facilitate detection, investigation and successful prosecution of criminals involved in these transnational illegal activities. Close cooperation between the local law enforcement agencies and the private sector, such as banks, could also lead to early detection and apprehension of the culprits. In the 3 cases of telegraphic transfer fraud mentioned earlier, the close coordination between the UK, US law enforcement agencies, the local banks and the Singapore Police resulted in the arrest of the culprits.

VI. COMPUTER CRIME

A. Introduction

Commercial and non-commercial organisations increasingly realize the strategic potential of Information Technology (IT) and they use IT to gain competitive advantage in the rapid changing global environment. IT enables business enterprises to compete globally and ensures that we will enjoy a higher quality of life. Unfortunately, the progress of IT also enables criminals to commit a whole new range of high-technology crimes eg computer hacking, unauthorized access, and sabotage of computer materials. Organized crime syndicates also employed IT to facilitate commission of traditional offences such as forgery, cyber gaming and prostitution.

B. Computer Crime in Singapore

A global definition of computer crime has not been achieved. In Singapore, what constitutes computer crime is defined under the Computer Misuse Act, enacted in August 1993. There are four main offences under this Act, namely, unauthorised access to computer material (eg. hacking), unauthorised access to commit further offences involving property or fraud, unauthorised modification of computer material (eg. introduction of viruses) and unauthorised use/interception of computer service (eg. unauthorised use of other's Internet account). The Act was amended in middle of 1998 to include another two offences, namely, unauthorised obstruction of use of computer and unauthorised disclosure of access code for any wrongful gain or for unlawful purposes.

There are other computer-related crimes where a computer is used as an instrument in committing crimes. These cases are dealt with under other existing legislation, for example, the Penal Code. The number of computer crime cases in Singapore is relatively low compared to other crimes. However, the numbers are increasing over the years. In 1993 and 1994, only 1 case was reported. In 1995, only 3 cases were reported. The number of cases reported more than doubled in 1996 to 7 and the increase was more than 5 times in 1997 to 38 cases. Until the middle of 1998, 39 cases have been reported and the figures are still increasing (table 1). Although the majority of these cases are unauthorised access to obtain computer service, committed by teenagers, there are a few cases of economic computer crime which resulted in significant losses.

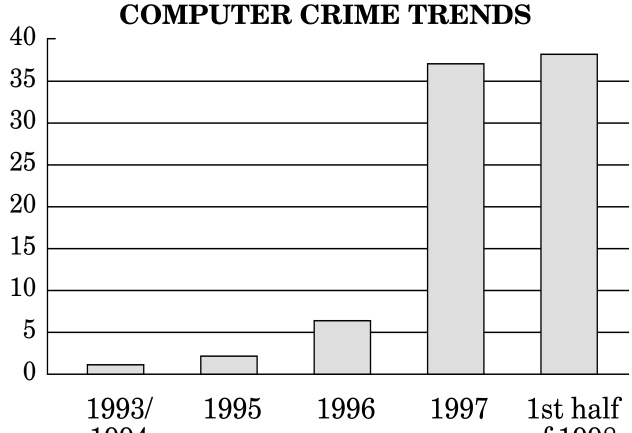
Most of the economic computer crime were perpetrated by employees of the victimised companies. Some examples include a case where an ex-employee of a bank siphoned away S$1.2 million from the bank. In this case, the ex-employee was allowed entry into the working area of the bank manager and left alone to move freely. He managed to find an unattended terminal, keyed in his account number and bank over-riding codes, and credited a sum of S$1.2 million into his account. He knew the bank's over-riding code through 'shoulder surfing'. (i.e. peeping over the officer's shoulder to observe the keying in of the over-riding code). Later in the same day, he withdrew the entire sum of S$1.2 million and fled from Singapore. He was eventually arrested in Malaysia and extradited. He was charged in court and sentenced to five years' imprisonment. In another case, an employee gained access to the payroll system and credited more than S$30,000 to his own salary. This was not detected until three years later.

In another case involving smart card technology reported in early 1997, two managers of a major cinema chain modified the cinema's ticketing system to siphon off cash amounting to about S$500,000. The managers were convicted and sentenced to 36 months and 24 months' imprisonment. A Computer Service Engineer who assisted the manager to illegally modify the computer system, was also convicted and sentenced to one month's imprisonment.

Sabotage of companies' computer systems usually occurs when the offender is unhappy with the company management. In one such case, a disgruntled System Administrator inserted a Trojan horse program that replaced the original system files with damaged files while the back up of the system was done. He also used a logic bomb program to time the back up process so that he would not be in the country at that point of time. As a result, the company's system crashed and the entire manufacturing process came to

TABLE I

COMPUTER CRIME TRENDS



a stand still. The offender was convicted under the Computer Misuse Act and fined S$20,000.

The profile of criminals committing cases of unauthorised access commonly known as 'hacking' is quite different from criminals who commit economic computer crime. Generally, hackers are teenage students. They usually commit unauthorised access to a computer system for kicks, without further criminal intent. Our Computer Crime Branch has solved cases where students 'hacked' into local and overseas servers for free access to the Internet. They obtained the knowledge of 'hacking' through the Internet or from friends. The technical knowledge of a computer criminal varies from novice to professionals (e.g. with tertiary education in computer related subjects). In our experience, computer criminals are often bright, serious and relish a technical challenge, but they are not geniuses.

C. Countermeasures

Cyberspace will present new opportunities for criminals and change the modus operandi of crime. This has implications on the strategies and capabilities required for detecting, enforcing and preventing of crime. The integrity of the social and economic environment in which law enforcement agencies operate is therefore likely to be affected by these characteristics in the new millennium. Countermeasures implemented to fight computer crime include the following:

(i) Expertise in criminal investigation;
(ii) Preventive measures;
(iii) Detection measures;
(iv) Legislation; and
(v) Partnerships and International co-operation.

1. <u>Expertise in Criminal Investigation</u>

The Singapore Police Force has responded to this challenge as early as 1981 when an officer was sent to the FBI Academy, USA, for training in computer crime investigation. Since then, officers have been sent to the USA, UK, Canada and Hong Kong for training and attachment. To further enhance our capabilities, the Computer Crime Branch of CID was set up in January 1997 to handle the investigations of computer crimes and to conduct computer forensic examination. Most of the officers of the Computer Crime Branch have received formal education in computer studies. They were also trained locally by professional trainers from the USA and UK to handle computer forensic examination.

Criminals who commit high-technology crime usually leave behind electronic fingerprints. We start by asking, "What needs to be done?" in order to leverage on the opportunities provided by IT. Our experience shows that electronic fingerprints has helped the investigation agency to solve crimes. We must take on the challenge of technology and develop capabilities to retrieve and examine these electronic fingerprints.

2. <u>Preventive Measures</u>

The importance of IT security is always neglected by the users. Generally, there is a lack of security standards for those systems operating in cyberspace. A sound security system will deter, if not reduce, the incidence of computer crime. Public education is a means to bring security awareness to the community. Towards this end, our National Computer Board and the Computer Crime Branch have held regular seminars and talks to highlight the importance of computer security to the industry.

3. Detection

Most of the computer crime cases are either not detected or are discovered sometime later. In one of the cases highlighted earlier, the offence was only discovered three years later. In our public education seminars/talks, we constantly remind the business community to adopt security practices to detect the occurrence of crimes. Such measures include physical security, proper procedures and audit capabilities. Early detection of a crime will prevent the victim from suffering drastic losses.

4. Legislation

Legislation has to be constantly reviewed to ensure that it can keep up with technological progress and adequately deal with computer crime. The Computer Misuse Act was enacted in August 1993 to make provision for securing computer material against unauthorised access or modification. With the increasing use of computers, not only has the number of computer crimes increased, but new crimes have also come about. The Act was thus amended in July 1998 to enhance the penalties against computer criminals and provide stiffer penalties for repeat offenders. It also introduces new offences of unauthorised obstruction of use of a computer and unauthorised disclosure of access code for any wrongful gain or for any unlawful purpose. The concept of 'protected computers', which are systems used in connection with national security, banking and finance, emergency services and essential public services, was also introduced and offences committed against these systems would attract enhanced penalties. The tough laws will serve as a deterrent to potential computer criminals. In addition, the amended Act also provides additional police powers for investigation into computer crime.

5. Partnerships and International Co-operation

Law enforcement agencies needs to tap industry and academic expertise in the field of forensic computing. Information technology is wide ranging and no one person can profess to know everything about information technology. Partnering with various organisations having expertise in the related fields will complement our capabilities. We will need to liaise and employ the services of industry experts to retrieve and analyse evidence on proprietary devices or software.

There is also increasing need for countries to cooperate in the fight against computer and computer-related crimes. With the rapid expansion of large-scale transnational computer networks and the easy accessibility of many systems through communication lines, such crimes are easily committed on an international scale. A criminal can physically operate in one country, access systems in another country, and cause the consequences to be felt in a third country. Committed and concerted mutual co-operation and assistance can assist to combat transnational computer crimes more effectively. The commitment among nations to assist each other in investigation and prosecution can also resolve potentially complex issues of territorial jurisdiction, extradition and trans-border searches and seizures of electronic evidence.

VII. CONCLUSION

Organised economic crime and transnational computer crime can result in significant losses of revenue and resources. It could render the financial and legal systems vulnerable and diminish the Asia Pacific region's credibility as an investment and business hub. This would in turn adversely affect the region's economic wealth.

Effective responses are needed to counter organised economic crime and computer crime, both at the national and international levels. At the national level, a review of existing legislation may be necessary to address the difficulties in prosecuting cross-border criminals. Close cooperation between the police and private sector (e.g. banks, credit card service providers, IT service providers) would facilitate better exchange of information. This could lead to the early detection and apprehension of culprits.

On an international level, regional States should work closely with one another to fight economic and computer crime. This would facilitate investigation and prosecution of cross-border criminals. States would eventually recognise that policing is now carried out over a global community. In the region, there are currently conferences organised by regional groupings such as ASEANAPOL on cross-broder crime and enforcement concerns. Such regular meetings are helpful in fostering mutual understanding and cooperation. They may also enable regional States to map out long-term working relationships with one another.

In the next millennium, policing will be carried out over a borderless community, rather than within the confines of national boundaries. Therefore, Asia Pacific States should aim towards cultivating strong links in the areas of intelligence and operations. In this way, we can overcome the limits posed by such crimes' cross-border nature and speed at which the criminals work. We could then look forward to solving such crimes in a more effective and comprehensive manner.