For discussion
on 2 March 2000

Legislative Council Panel on Security

Computer-related Crimes

Purpose

This paper informs Members of the general situation regarding computer-related crimes, the enforcement difficulties faced and enforcement strategy to combat such activities.

An Overview

2. The number of reported computer-related crime cases has increased considerably from 34 cases in 1998 to 317 cases in 1999. Most of the cases are minor in nature. A breakdown of these reports since 1996, and the number of cases detected/convicted and persons arrested/convicted in the past two years are as follows -

Case Nature	**1996**	**1997**	**1998**	**1999**
Hacking	4	7	13	238

Publication of obscene articles	6	6	13	32
Criminal damage of data	4	3	3	4
Internet shopping fraud	0	2	1	18
Others	7	2	4	25
Total	**21**	**20**	**34**	**317**

	Cases Detected (No. of persons arrested)	**Cases Convicted (No. of persons convicted)**
1998	10 (22)	8 (19)
1999	18 (48)	5* (12)

*Among the 18 detected cases, seven are still pending.

3. Hacking is the most common category of computer-related crimes in Hong Kong. Most of the cases were motivated by a desire to beat the system security without causing major damages to the system. Hacking is characterised by inflated service charges to the account owners, which could be wrongly perceived as the result of system malfunction. Hence, the figure may be under-reported before 1999 when its awareness was lower. Hacking cases are expected to increase as more people become aware of hacking tools that are freely available

through the Internet and are for sale in hacking magazines with CD-ROMs. In addition, more sex sites and pornography are appearing on the Internet. Recent Internet statistics showed that 25% of all key word Internet searches relate to sex or pornography. However, enforcement of the law is hampered by jurisdictional problems when an obscene article is published on a web site that is 'hosted' overseas.

4. The increase in these reports corresponds generally with the increase in the use of the Internet in Hong Kong. By late 1999 there were:-

(a) 159 licensed Internet Service Provider (ISP) companies as compared to 3 in 1994 and 56 in 1995; and

(b) over 1.7 million registered Internet customer accounts as compared to 600,000 at the start of the year.

5. The majority of computer hackers, who are commonly young people, are motivated by curiosity rather than any genuine criminal intent. Whilst most of the computer-related crimes at present remain mischievous and relatively minor in nature, the greatest threat in the future is the adoption of information technology by organised crime groups to carry out illegal activities across national boundaries.

Existing Legislation

6. In 1984, a Working Group on Computer-related Crimes was

formed within the then Legal Department to consider the need for changes to the criminal law to counter computer-related crimes and the unauthorised accessing of computer systems. To implement the Working Group's recommendations, the Computer Crimes Ordinance was enacted in 1993 to amend the Telecommunication Ordinance (Cap.106), Crimes Ordinance (Cap.200) and Theft Ordinance (Cap.210). At present, the main statutory provisions that deal with computer-related crimes are :-

Law	Offence	Maximum Penalty
S. 27A, Cap. 106	'Unauthorized access to computer by telecommunication'	Fine of $20,000
S. 161, Cap. 200	'Access to computer with criminal or dishonest intent'	5 years' imprisonment
S. 60, Cap. 200	'Criminal damage to property', which applies to misuse of a computer program or data.	10 years' imprisonment

S. 11, Cap. 210	'Burglary', which includes unlawfully causing a computer to function other than as it has been established and altering, erasing or adding any computer program or data.	14 years' imprisonment
S.19, Cap. 210	'False accounting', which includes destroying, defacing, concealing or falsifying records kept by computer.	10 years' imprisonment
S. 21, Control of Obscene and Indecent Articles Ord. (Cap. 390)	'Publishing an obscene article', which applies to the display of obscene images on the Internet	3 years imprisonment and $1 million fine

Enforcement Difficulties

7. With the rapid development and wider application of information technology, the increasing popularity of Internet and the development of e-commerce, the complexity of investigations of computer-related crimes has intensified. Computers are no longer just a tool for committing crimes. They have become a target of crimes and have facilitated the commission of the so-called 'cyber crimes', i.e. crimes committed through Internet and takes place in the virtual or electronic environment of computer systems.

8. Law enforcement agencies encounter increasing difficulties in taking enforcement action against computer-related crimes, in particular in the following areas -

(a) Intangible environment: The cyber world is an intangible environment that is completely different from the physical world that the law enforcement agencies have been dealing with. For example, an information in electronic data form is not visible as a physical document containing the same information. A theft of data could be just copying of the data without depriving the owner of its ownership. In addition, a hacker can access from his home a target system which is far away. Hence, traditional skills adopted by law enforcement agencies in investigating crimes including the way of soliciting evidence will need to be adjusted. Existing legal concepts may also be inadequate to deal with all situations in the cyber world.

(b) Border free: The cyber world is without any boundaries. Computer-related crimes are beyond geographical boundaries. It is technically feasible to make use of a keyboard in Country A to alter data stored in Country B that leads to the fraudulent obtaining of goods in Country C. Investigations of these crimes may therefore give rise to jurisdictional problems and require transnational assistance. The disparity in legal standard between different jurisdictions also complicates the issue.

(c) Difficult differentiation between original and copy of a data: The advanced digital technology makes differentiation between the original article and a copy very difficult. Digital technology can transform data like music, movies, electronic cash, software and may other intellectual products and services into a bit stream. Investigation is difficult as the original and copy may be identical in all aspects.

(d) Misuse of data: With the wide application of information technology, a data bank such as data stored in a credit card generally contains a sizable volume of personal information. However, at present, unlike "property" in the conventional sense, there is no specific legislation dealing with misuse or unauthorised use of such data.

(e) Anonymity of offenders: As the virtual environment in the cyber world does not allow full identification of offenders in a physical and conventional fashion, proving an individual's involvement in an offence could be very difficult.

(f) Deception of a machine: According to the existing legal concept, an offence of deception requires the deception of a human. As computer systems have a role of decision making when a person makes an on-line purchase through the Internet, an offender of 'Internet Shopping Fraud' may argue that the deceiving act only targets a machine, not a human which hence is not an offence.

(g) Emergence of 'E-mail Spamming': This means flooding computers with multitudes of e-mail messages or sending large numbers of unwanted e-mail messages to many Internet users. Although such act causes nuisances and loss to the Internet users as they have to pay for the time to store and receive the messages, it is not a criminal offence at present.

(h) Encryption of data: Encryption technology has developed very rapidly and become more and more popular. Law enforcement agencies may not be able to retrieve seized data that have been encrypted by the owner.

(i) Record retention: Under the existing licensing conditions, ISPs are not required to retain records for a certain period of time. These records are valuable information that can facilitate investigations.

Enforcement Strategy

9. The magnitude, dimension and changing scene of computer-related crimes is being closely monitored so that appropriate counter measures can be taken timely. The following strategies are being pursued by the Police Force to face the challenges of computer related crimes :-

(a) Maintaining a professional capability of investigation into computer related crimes, with continuous improvement to keep up with the advance in technology.

(b) Broadening the investigation capability within the Police Force so that frontline formations are able to respond to these investigations, leaving complex and serious cases to more specialised formations.

(c) Development of an accredited capability of professional computer forensic examination.

(d) Review of the laws with a view to strengthening legal powers for countering computer related crimes.

(e) Raising public awareness on computer related crimes and computer security with the assistance of other agencies and government departments where necessary.

(f) Liaison with the industry including the ISPs and professionals for enhancing understanding and intelligence gathering on illegal cyber activities and for monitoring the development of information technology in order that countering measures against computer related crimes be improved.

(g) Liaison with overseas authorities and law enforcement agencies for mutual cooperation against computer crime, and exchange of intelligence on and expertise against the problem.

10. A Computer Crime Section (CCS) has been set up within the Police Commercial Crime Bureau (CCB) since 1993 for the investigation of computer-related crimes. For the purpose of broadening the investigative capability in the Police Force, a Computer Crime Investigation Cadre (CCIC) comprising 83 officers from various districts and other formations has also been formed since December 1999. They will assist in computer crime investigation in frontline formations in terms of examination of computers, including seizure of exhibits. CCS will coordinate their deployment, provide the necessary technical support to these investigations and deal with the more serious or transnational cases.

11. The CCS is also responsible for the centralised forensic examination of computer systems involved in crimes that are investigated by other formations throughout the Force. The examination aims to recover crime evidence from the systems for proving the relevant offences. The results of the examinations may be tendered in evidence in court trials if required. At present, there is no international standard for such examination. The need for due accreditation of computer forensic examiners and setting standards of computer forensic examination is therefore required. A Computer Forensic Examination Working Group involving the Hong Kong University of Science and Technology (HKUST), the Police Force and the ICAC has been initiated since late 1998. A professional computer forensic training program with an internationally recognised Standard of Practice will be formulated. The expertise in computer forensic examination will be further developed along with the advance in technology.

12. Members of CCS and CCIC have received basic training on computer forensic examination. A Computer Crime Investigation and Computer Forensic Examination Course which is an advanced course and aims at training the trainers ran between 7 and 25 January 2000. Academics from HKUST, the University of Hong Kong and the City University were involved in providing the training. It was attended by 23 officers from the Hong Kong Police Force, the Independent Commission Against Corruption, Customs & Excise Department, Immigration Department and the Department of Justice. The training, which is the first of its kind in Asia, will be accredited by the HKUST. It will also form part of a post-graduate course in Masters Degree in Information Technology Management. As the course is well-received by the participants, it is envisaged that at least two more courses will be held this year.

13. A 'Computer Security Unit', being part of the Police Crime Prevention Bureau, has been set up for providing computer crime prevention advice to companies, schools and individuals. Further measures to raise public awareness on the computer crime problem are conducted by the CCS. A list of these activities is at **Annex.**

Review of Legislation

14. To overcome the enforcement difficulties mentioned above and effectively combat the growing computer related crimes, law enforcement agencies will need additional legal powers and new criminal offences. An inter-departmental working group, chaired by the Security

Bureau and comprising representatives of the Information Technology & Broadcasting Bureau (ITBB), Department of Justice, law enforcement agencies and other concerned bureaux/departments will shortly be set up to examine the existing legislation on computer-related crimes.

Involvement of Other Departments

15. The Department of Justice has established a new computer crime section within the Commercial Crime Unit of the Prosecutions Division since January 2000. Its primary duties include the provision of legal advice to law-enforcement agencies regarding criminal charges to be laid in the area of computer-related crimes and the actual conduct of such prosecutions in the Courts. To enhance its effectiveness, the team will liaise regularly with local law enforcement agencies and international prosecution agencies. The team will also attend conferences and training courses devoted to combating computer-related crimes.

16. As one of the initiatives of ITBB to promote the development of e-commerce in Hong Kong, ITBB is seeking to develop a secure environment for the conduct of electronic transactions over open computer networks through the establishment of a public key infrastructure, to be supported by the operation of certification authorities. With the issue of digital certificates by certification authorities and the use of digital signatures and public/private key technology, participants in e-commerce will be able to authenticate the identity of opposite parties in electronic transactions, ensure the integrity and confidentiality of electronic messages exchanged in the transactions,

and safeguard the non-repudiations of the transactions made with these messages. These will help to reduce computer-related crimes relating to the use of false identity for deception purposes in electronic transactions or the interception of electronic messages to gain access to private information for criminal use.

17. The Electronic Transactions Ordinance was enacted by the Legislative Council on 5 January 2000. The Ordinance, inter alia, establishes a framework to facilitate the development of certification authorities in Hong Kong and gives legal recognition to electronic records and digital signatures as that of their paper-based counterparts. The Hongkong Post has taken the lead in providing certification services. Its certification authority project was launched on 31 January 2000 to provide services to both individuals and businesses.

18. ITBB and Hongkong Post (HKP) will continue to carry out promotional and publicity activities to educate the public on the benefits of the public key infrastructure in enhancing the security of electronic transactions through exhibitions, seminars and workshops. HKP and the Hong Kong Productivity Council (HKPC) have also jointly established a Promotion and Support Centre to promote the use of certification services among small-and-medium sized enterprises through the distribution of relevant information and the organisation of seminars on a regular basis. In addition, the Information Technology Services Department (ITSD) has organised other publicity activities to raise public awareness on computer security and the proper use of the Internet-

(a) a forum on 'Explore IT with Kids' was held in conjunction with the Education Department to launch an education campaign on the use of the Internet for parents of secondary school students;

(b) a plan has been drawn up to launch a programme similar to that designed for secondary schools in (a) for primary schools;

(c) in November 1999, in association with the Police and the HKPC, ITSD held a seminar on Internet security and computer crime for the IT industry;

(d) another information security seminar/exhibition is being organised together with the HKPC to be held in April this year. This will be an information security showcase for information security solution providers to exhibit their products and services such as intrusion detection devices, firewall, cryptograph, virus detection devices, etc. It will target at organisations with computer systems, particularly systems with network and Internet connections. Special focus will also be placed on addressing the needs of small and medium sized enterprises; and

(e) the publication of the Government's own information technology security standards and guidelines at the Department's web site for the public's reference.

19. With the support of the Office of the Telecommunications

Authority (OFTA) and the Office of the Privacy Commissioner for Personal Data, the Hong Kong Internet Service Providers Association has recently published a code of practice on anti-spamming for the members of the Association to follow. The code sets out that sanctions such as suspension of services should be imposed on spammers and that preventive measures should be taken by ISPs to reduce the possibility of spamming. The use of administrative measures to tackle spamming has the support of the Information Infrastructure Advisory Committee, the Privacy Commissioner for Personal Data and the ISP industry.

20. Separately, the OFTA has also published, in consultation with the Association and the Privacy Commissioner, a promotional leaflet on "Frequently Asked Questions on Spam", which contains useful tips for Internet users to minimise the nuisance of receiving spam. The leaflet is available from all District Offices, major Post Offices and the homepage of OFTA.

Security Bureau

February 2000

[p-computer.doc]

Annex

Measures To Raise Public Awareness Of Computer Crime

- Frequent briefings to the press and members of the media.

- Presentations to private and public organisations regarding computer crime and its impact in Hong Kong. Organisers of these forums include the Security Association of HK, Federation of HK Industries, the HK Productivity Council, and school headmasters (organised through the Education Department).

- Building partnerships with local universities to develop their interest in computer crime research and prevention through IT development.

- Development of an intelligence network amongst local corporations and organisations to enhance the reporting of computer crime to the police and the ability of the participants to better prevent and detect computer crime attacks.

- The Crime Prevention Bureau (CPB) advises the public on possible victimisation of computer crime and promotes security of computer systems. Its functions are publicised in the CPB web site at http://www.infor.gov.hk/police/cpb.

- A manual for Users of Small Computer Systems has been issued to advise on systems security since 1997.

- Publicity materials including mouse pads and stickers promoting good computer security practices have been issued.

- Publicity booths were set up in two major computer related exhibitions at the HKCEC in May and November 1999. The events attracted a high volume of attendees.

- In response to growing concerns from parents and teachers over the potential problems of children using the Internet, school talks were conducted and a pamphlet promoting protection of children online has been produced.

- CPB has participated in an ITSD/Education Department project to produce a video on ‘IT awareness for parents’.

- The Police Public Relations Bureau (PPRB) has produced two computer related crime features in 1998 and two more in 1999. Officers from the CCS have taken part in the presentations to highlight to the public the problems with computer related crimes.