Inter-departmental Working Group on Computer Related Crime

Report

We welcome your views

It is always the Government's aim to ensure that our response to crime can keep pace with the demands of changing circumstances. The Inter-departmental Working Group on Computer Related Crime was established in March 2000 with this in mind. The Working Group submitted its report in September 2000. Its report is now released for public consultation.

As use of the computer and the Internet increasingly affects our daily pursuits, we welcome your views on the report. Comments on the report should be sent, by 31 January 2001, as follows –

- *by post : Security Bureau*
  (Attn. : CAS, F Division)
  6th Floor, East Wing
  Central Government Offices
  Lower Albert Road
  Central

- *by fax : 2521 2848*

- *by e-mail : sbcassf@sb.gov.hk*

You are encouraged to let us have your comments by e-mail if possible to reduce paper consumption. Nonetheless, should you prefer to post your comments to us, we have prepared the address label at the bottom of this page for your convenience.

Copies of the report are available at all District Offices and may be accessed at the Security Bureau website at www.info.gov.hk/sb/ or through the Government Information Centre website at www.info.gov.hk/eindex.htm. As far as possible, you are encouraged to access the report through these websites in order to reduce paper consumption.

For enquiries, please contact Mr John Lee of the Security Bureau on 2810 2973.

Security Bureau
(Attn. : CAS, F Division)
6th Floor, East Wing
Central Government Offices
Lower Albert Road
Central

Inter-departmental Working Group on Computer Related Crime

Report

September 2000

Table of Contents

Annexes **Pages**

Summary of Recommendations

The recommendations of the Working Group are summarized below.

Defining "Computer" in Law

1. There is merit in setting out in our law some parameters within which the concept of "computer" should be interpreted. The term "information system" as defined in the Electronic Transactions Ordinance (Cap. 553) should be used in place of the term "computer" (paragraph 3.9). In principle, to ensure consistency, this amendment should apply across the board to all references to the term "computer" in our legislation (paragraph 3.10).

Jurisdiction

2. Consideration should be given to conducting a thorough in-depth study of the subject of jurisdictional rules in general to take account of the greatly increased ease of transportation and communications (paragraph 4.10).

3. The following offences, as modified to take into account the recommendations in this Report, should be covered by the Criminal Jurisdiction Ordinance (Cap. 461) –

   – unauthorized access to computer by telecommunication (S. 27A, Telecommunications Ordinance (Cap. 106)); and

   – access to computer with a criminal or dishonest intent (S. 161, Crimes Ordinance (Cap. 200))

   (paragraphs 4.15 and 4.17).

Encryption

4. Legislation should be introduced to enable law enforcement agencies to be provided with the decryption tool or the decrypted text of encoded computer records where necessary and justified (paragraph 5.14).

5. The compulsory disclosure requirement should be subject to judicial scrutiny (paragraph 5.18). A process similar to that for applying for "production orders" under Section 4 of the Organized and Serious Crimes Ordinance (Cap. 455) should be adopted for the purpose (paragraph 5.22).

6. The disclosure power should apply to offences of a more serious nature. Only offences attracting a maximum penalty on conviction of not less than, say, two years' imprisonment should be subject to the disclosure requirement (paragraph 5.25).

7. There should be suitable legal protection of the confidentiality of the information obtained through the disclosure procedures. The evidence obtained as a result of compulsory disclosure should be admissible in court (paragraph 5.26).

8. The penalties for non-compliance with the disclosure requirement should in principle be commensurate with those for the specific offence under investigation (paragraph 5.27).

Protection of Computer Data

9. Existing legislative provisions on unauthorized access to the computer, while covering much of what needs to be protected in terms of computer data, should be further improved (paragraphs 6.18 and 6.19).

10. All computer data at all stages of storage or transmission via a computer or the Internet should be covered (paragraph 6.19).

11. The term "access to computer" should be clarified to include access to a computer as well as the programs and data stored therein (paragraph 6.19).

12. Unauthorized access to the computer by any means instead of by telecommunication only should be unlawful (paragraph 6. 19).

13. Receiving, retaining and handling/trafficking of computer data known to have been obtained through unauthorized access to the computer should be prohibited (paragraph 6.19).

14. It should be illegal to sell, distribute and make available any computer password or access code for wrongful gain for oneself or another, an unlawful purpose or causing wrongful loss to another (paragraph 6.19).

15. It is unnecessary and impracticable to legislate against hacking tools. The proposal should not be pursued (paragraph 6.23).

16. It is necessary for any anomalous situation between the treatment of computer data and physical data to be studied and rectified as appropriate (paragraph 6.25).

"Deception" of Computers

17. Existing legislation is adequate to deal with "deceptions" of computers (paragraph 7.9). However, consideration should be given to studying and rectifying the gap in our law where at present the "deception" of a machine other than a computer is not an offence (paragraph 7.10).

Penalties for Offences

18. The penalty for unauthorized access to the computer should include a custodial term. A sufficient deterrent should not be less than that for theft (paragraphs 2.7 and 6.22).

19. The current penalty of 5 years' imprisonment for accessing a computer with the intent to commit an offence, S. 161(1)(a) of the Crimes Ordinance (Cap. 200), should be amended, to the effect that it should be decided having regard to the severity of the offence to be committed (paragraph 4.16).

20. The current penalty of 5 years' imprisonment for the deception and dishonest intent parts of S. 161 of the Crimes Ordinance (Cap. 200) (i.e. S. 161(b), (c) and (d)) should be amended, so that the maximum sentence will not be less than 10 years (paragraph 7.11).

Assistance from Internet Service Providers (ISPs)

21. The existing practice of tracing the transactions of specific accounts suspected of involvement in computer crime on a need basis only should continue (paragraph 8.22).

22. ISPs should be encouraged to keep log records including the calling numbers as a good management practice. However, the proposal to impose a mandatory requirement for all Internet transactions to be tracked by the caller line identification function or caller number display function should be put on hold (paragraph 8.22).

23. Administrative guidelines on record-keeping by ISPs should be drawn up to cover, among others –

- subscriber details to be inspected on opening of an account and those which should be kept;

- details to be captured by log records – these should include at least the time of logging in and logging out as well as the Internet protocol address assigned for an Internet transaction, and preferably the caller number; and

- the period for which records should be kept – say, six months,

to facilitate computer crime investigation (paragraphs 8.16, 8.24 and 8.26).

24. The guidelines should be drawn up in consultation with ISPs (paragraph 8.26.)

25. The guidelines should be given suitable publicity. Consumers should be encouraged to choose ISPs who adopt the good management practices set out in these guidelines (paragraph 8.27).

26. Internet users should be encouraged to make use of the Public Key Infrastructure for enhanced security, although the requirement should not be made mandatory (paragraph 8.23).

27. In principle, take-down procedures for ISPs to remove offending materials should be endorsed. The relevant Policy Bureaux should examine the feasibility of putting in place such procedures in respect of copyright protection, Internet gambling and pornographic materials (paragraph 8.30).

28. ISPs should be encouraged to set their system default to deny multiple log-in, and instead offer the facility only as an option (paragraph 8.31).

29. The market-led approach for dealing with credit limits for on-line shopping should continue. There is no need for legislation to require ISPs to set limits on credit card payment transactions through the Internet (paragraph 8.32).

30. Communication between law enforcement agencies and ISPs should be enhanced by –

- establishing a forum of exchange for both sides to discuss matters of mutual concern at the macro level at regular intervals; and

- setting up a contact point system for ISPs and law enforcement agencies for dealing with computer crime investigation requests (paragraph 8.33).

Protection of Critical Infrastructures

31. A thorough risk assessment of our critical infrastructures vis-à-vis cyber attacks should be undertaken (paragraph 9.16).

32. A standing central mechanism capable of coordinating the preparation and synchronization of protection, contingency and recovery plans against computer and Internet-related security threats to our critical infrastructures should be established (paragraph 9.17). The emphasis of this mechanism should be on better coordination across the board in terms of threat and vulnerability assessment, and preparation and regular updating of protection, contingency and recovery plans, both individually and collectively (paragraph 9.18).

33. The Emergency Response System exercises mounted by the Government should include scenarios of cyber attacks to our critical infrastructures (paragraph 9.17).

34. From the point of view of law enforcement facilitation, the setting up of a computer emergency response team (CERT) is supported (paragraph 9.21).

35. Our critical infrastructure operators should be covered by the CERT if and when it is set up (paragraph 9.22).

36. Pending the establishment of the CERT, liaison has to be increased between the Information Technology Services Department and critical infrastructure operators to enable the prompt sharing of information to better deal with emergency situations (paragraph 9.22).

Public Education

37. There should be a mechanism involving all Government departments and other public sector organizations which are currently engaged in education or publicity efforts on information security to –

- provide a common forum for sharing information;

- facilitate cross-agency participation in and contribution to each other's programs;

- serve as the focal point for mapping out the public sector's overall education and publicity strategy on information security; and

- coordinate the mobilization and involvement of the private sector in public sector-led programs on information security, and vice versa

(paragraph 10.7).

The Private Sector's Role

38. The market-led approach in developing information security devices or programs should continue (paragraph 11.5).

39. The law enforcement agencies should share with the relevant industries information obtained from computer crime investigation on how security has been breached. The private sector should keep the law enforcement agencies abreast of trends and developments in information security and share their security concerns (paragraph 11.6).

40. The private sector itself should organize information sharing initiatives on information security issues (paragraph 11.6).

41. The private sector, in particular, professional organizations, industry associations and chambers of commerce, should be encouraged to undertake more education and publicity efforts on information security at various levels (paragraphs 11.7 and 11.8).

42. Government and public sector agencies should lend as much support to private sector-led publicity and education initiatives on information security as possible. Similarly, they should actively involve the private sector in their own education efforts (paragraph 11.9).

43. The Government should continue to involve the private sector in the formulation of policies on computer crime and seek its input on a more regular basis (paragraphs 11.10 and 11.11).

44. The feasibility of a commonly accepted audit or assessment mechanism to certify the information security standards for different industries and at different levels should be explored (paragraph 11.12).

Resources and Capabilities

45. Sufficient resources should be provided for the effort to combat and prevent computer crime (paragraph 12.17).

46. The law enforcement agencies should continue to closely monitor the availability of computer crime investigation and computer forensic examination expertise to ensure that there is no mismatch between demand and supply. Private sector resources and cooperation should be leveraged on as far as possible (paragraph 12.18).

47. The proposal for pooling all law enforcement resources in respect of computer crime to form a central one-stop unit should not be pursued (paragraph 12.19).

48. The cooperation and sharing of intelligence and experience between the law enforcement agencies should continue and be deepened (paragraph 12.20)

49. The law enforcement agencies should step up their liaison with their counterparts outside Hong Kong (paragraph 12.21).

50. Our law enforcement agencies should keep close tabs on international developments regarding procedures for handling computer evidence to ensure that Hong Kong's procedures are in line with the international standards once they are available (paragraph 12.22).

51. A standard set of procedures for handling computer evidence among all law enforcement agencies in Hong Kong should be worked out as soon as possible. The soon to-be-established Police Computer Forensic Laboratory should take the lead in developing this common standard (paragraph 12.23).

52. Once the common standard for handling computer evidence is developed, it should be publicized among judges, the legal profession and other interested parties (paragraph 12.23).

53. In the longer run, consideration should be given to establishing a computer forensic examination unit or laboratory to provide computer forensic service centrally (paragraph 12.24).

Future Institutional Arrangements

54. A sub-committee under the Fight Crime Committee should be formed to follow up on the Working Group's proposals, monitor relevant developments as they evolve and assess their impact on our policies and measures (paragraph 13.8).

55. The sub-committee should include, among others, senior representatives of law enforcement agencies and some private sector representation (paragraph 13.9).

Others

56. In general, new legislation or amendments to existing legislation should be drawn taking into account the requirements of the information age. As far as possible, legislation should be technology- and medium-neutral (paragraph 14.4).

57. To maximize public acceptance and cooperation, interested parties should be consulted when details of implementing the Working Group's recommendations are being mapped out (paragraph 14.5).

Chapter I

Background and Approach

Introduction

1.1 The growth in Internet and computer use over the past few years has been phenomenal. This has brought about much speed and convenience in our daily pursuits – learning, communication, leisure and business etc. At the same time, this has created the potential for abuse by criminals. An increase in computer related crimes(1) is a cause for concern internationally.

1.2 In Hong Kong, the number of computer crime reports handled by the Police and the Customs and Excise Department increased from 21 cases in 1996 to 318 cases in 1999(2). A breakdown of the cases reported since 1996 is as follows –

Case Nature	1996	1997	1998	1999	2000 (Jan-Jun)
Hacking	4	7	13	238	168
Publication of obscene articles	6	6	13	32	0
Criminal damage of data	4	3	3	4	6
Internet shopping fraud	0	2	1	18	11

(1) The terms "computer crime" and "computer related crime" are commonly used interchangeably to refer to crimes committed via the computer or the Internet. Please see para. 2.1, Chapter II, for more details. We will look into the question of whether a more precise legal definition of the term "computer" is required in Chapter III.

(2) The number of computer crime cases handled by other law enforcement agencies is negligible.

Case Nature	1996	1997	1998	1999	2000 (Jan-Jun)
Infringement of copyright	N.A.	N.A.	N.A.	1	43
Others	7	2	4	25	22
Total	21	20	34	318	250

The Working Group

1.3 Against this background, the Inter-departmental Working Group on Computer Related Crime (the Working Group) was established in March 2000. Our terms of reference are set out at **Annex 1**. The Working Group is chaired by the Security Bureau. Core members of the Working Group include representatives from various Government bureaux and departments. The full membership list of the Working Group is at **Annex 2**.

1.4 The Working Group held a total of six formal meetings between March and August 2000. In addition, numerous discussions were held amongst Working Group members themselves as well as between Working Group representatives and interested parties in the private sector (e.g., Internet service providers), academia and relevant statutory organizations. Some of us have also visited the United States, and discussed with relevant government agencies, other organizations and individuals there their views and experience of the various issues involved. Moreover, we have briefed the Information Infrastructure Advisory Committee(3) on our work and invited committee members' views. Given that the Working Group is an internal government task force, and that our recommendations will need to be scrutinized internally before they are implemented, we have not conducted formal full-scale public consultation as such. Nonetheless, we have benefited immensely from

(3) Please see para. 13.6, Chapter XIII.

discussions with non-Government parties, and we would like to express our most sincere thanks for all the suggestions and comments given us, and for all the assistance rendered us during the past six months. They have been invaluable in helping us to weigh the many different considerations involved and to frame our recommendations.

Approach

1.5 The Working Group's focus is strengthening the framework or environment within which law enforcement against computer crime may be carried out. We have therefore attempted to identify problems and recommend solutions, legislative or otherwise, regarding crime prevention, evidence gathering, investigation and prosecution arising from computer crime. Our ultimate aim is to contribute to the total effort of providing an environment conducive to the legitimate use of the computer and the Internet.

1.6 Our approach is a macro one by identifying solutions that may be applied across the board as far as possible. We therefore do not seek to deal with all crimes that may be committed via the computer or the Internet. These should continue to be considered in the relevant policy context. For example, consideration of Internet gambling is part of the overall policy consideration of gambling in general, and should appropriately be dealt with in that context. However, in so far as our recommendations will strengthen or facilitate law enforcement against computer crime, they also have a bearing on these specific crimes.

1.7 In making our recommendations, we have always been mindful of the need to balance law enforcement facilitation on the one hand and the likely cost of compliance on the other hand. We have favoured administrative measures over legislation where feasible, and have taken care to ensure that sufficient safeguards are available where additional legislative powers are proposed. As the Internet knows no borders, the Working Group has also taken into account relevant international developments and trends as an integral part of our deliberations.

1.8 The Working Group was tasked to complete its work within about six months' time. In the course of our deliberations, we have identified issues which require much more in-depth study than this timeframe would allow. In these cases, we have endeavoured to set out the basic framework within which the subject should be further pursued. Where immediate relief is deemed necessary, we have suggested possible measures for the purpose.

1.9 We have also identified issues falling outside the Working Group's purview which require follow up either on their own or as a consequence of implementing our recommendations. We will draw attention to these issues as we come across them.

Chapter II

Existing Legislation

Introduction

2.1 The terms "computer crime" and "computer related crime" are rather amorphous descriptions commonly used interchangeably to refer to any of the following –

(a) crimes directly targetted at the computer or computer system (e.g., computer intrusions commonly known as hacking);

(b) crimes using the computer as the medium (e.g., Internet gambling); and

(c) crimes where the computer may merely be incidental to the offence (e.g., placing an advertisement on the Internet to attract customers to buy pornographic articles at a bookshop).

The Working Group's main concern is category (a) as well as category (b) as a whole (as opposed to specific crimes)[4]. Crimes belonging to category (c) have only a tangential and incidental relationship to the computer, and should be more appropriately dealt with in other contexts. They are only relevant to our present consideration insofar as their investigation involves general issues such as encrypted computer records.

Overview

2.2 The main piece of legislation which has been introduced against computer related crime is the Computer Crimes Ordinance. Enacted in 1993, it has, through amending the Telecommunications Ordinance

(4) Please see para. 1.6, Chapter I.

(Cap. 106), Crimes Ordinance (Cap. 200) and Theft Ordinance (Cap. 210), created some new offences and broadened the coverage of existing offences, as follows.

Law	Provisions	Maximum Penalty
S. 27A, Cap. 106	prohibiting unauthorized access to computer by telecommunication	Fine of $20,000
S. 59, Cap. 200	extending the meaning of property to include any program or data held in a computer or in computer storage medium	Not applicable
S. 59 and 60, Cap. 200	extending the meaning of criminal damage to property to misuse of a computer program or data	10 years' imprisonment
S. 85, Cap. 200	extending the meaning of making false entry in bank book to falsification of the books of account kept at any bank in electronic means	Life imprisonment
S. 161, Cap. 200	prohibiting access to computer with criminal or dishonest intent	5 years' imprisonment
S. 11, Cap. 210	extending the meaning of burglary to include 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	extending the meaning of false accounting to include destroying, defacing, concealing or falsifying records kept by computer	10 years' imprisonment

2.3 In addition, many other legislative provisions refer to "computer" or similar terms. Some examples are set out below.

Law	Provisions
S. 20, Evidence Ordinance (Cap. 8)	making copy of entry in banker's record kept by means of a computer acceptable as evidence
S. 22A, Cap. 8	making documentary evidence from computer records acceptable in criminal proceedings
S. 54, Cap. 8	including computer generated records within the meaning of "records"
S. 2, Securities (Insider Dealing) Ordinance (Cap. 395)	including in the definition of "document" any form of computer input and output
S. 2, Land Survey Ordinance (Cap. 473)	including in the definition of "field note" a print-out from an electronic data recorder
S. 4, Copyright Ordinance (Cap. 528)	including computer programs within the meaning of literary works, which are in turn copyright protected works
S. 26, Cap. 528	including the making available of copies of copyright works via the Internet as acts restricted by copyright
S. 93, Patents Ordinance (Cap. 514)	providing that a program for a computer is not a patentable invention
Electronic Transactions Ordinance (Cap. 553)	giving electronic records and digital signatures the same legal status as that of their paper based counterparts
S. 10, Protection of Non-Government Certificates of Origin Ordinance (Cap. 324)	empowering an authorized officer to demand any information contained in a computer to be produced in a form which can be taken away and which is either visible or legible

Law	Provisions
S. 83, Securities Ordinance (Cap. 333)	creating an offence for any person who wilfully stores false material particulars or falsifies any entry or destroys records in an electronic device
S. 13B, Smoking (Public Health) Ordinance (Cap. 371)	prohibiting the placing of tobacco advertisements on the Internet

2.4 In many cases, although no explicit reference to the cyber environment is made, the relevant legislation may be interpreted to cover both the physical and the virtual worlds. For example, the provisions of the Personal Data (Privacy) Ordinance are equally applicable to the cyber environment as the physical environment.

Review

2.5 The Working Group has reviewed the legislative changes effected by the Computer Crimes Ordinance (para. 2.2 above). We believe that their ***thrust*** is still ***along the right lines***. In particular, the two new offences of unauthorized access to computer by telecommunication (S. 27A, Cap. 106) and access to computer with criminal and dishonest intent (S. 161, Cap. 200) have enabled many cases of reported computer crime to be dealt with. By and large, the new or extended offences created by the Computer Crimes Ordinance should continue to be kept.

2.6 In Chapters III to VII, we will discuss various legal issues involved with computer crime. We will examine in greater detail in that context whether and how some existing legislative provisions should be changed or improved to dovetail with our recommendations.

2.7 At this early stage, therefore, we will only restrict ourselves to a readily ***noticeable inadequacy***. This relates to the penalty for the hacking offence under S. 27A of Cap. 106 (please see para. 2.2). At present, the offence attracts a maximum penalty of only a $20,000 fine. Given the very significant damage that hacking may bring about, the Working

Group considers that the penalty is a woefully inadequate deterrent. We ***recommend***, therefore, that the penalty for that offence should include a custodial term. We will look into the related issues in greater detail in Chapter VI.

2.8 The Working Group has considered if all the legislative changes proposed in this Report should be captured in one ordinance. This might be more user-friendly than effecting changes to a number of existing ordinances. At the same time, we recognize that the use of the computer and the Internet is becoming almost ubiquitous. This argues more for taking the use of information technology as a given in our legislation in general than setting it apart (please also see Chapter XIV). As long as the intention and substance of the proposed changes are clear, therefore, we will leave it to the law draftsman to decide on the most appropriate legislative vehicle for effecting the proposed changes.

Chapter III

The Meaning of the Term "Computer"

Introduction

3.1 At present, the terms "computer" and "computer systems" are largely undefined in law, and are left to be interpreted by the court. Whilst they will continue to be used as handy shorthand expressions in the rest of this Report, we examine below the need for providing for a more consistent definition of the terms in law.

Existing legal definitions

3.2 At present, under Hong Kong laws, the term "computer" is defined in S. 22A of the Evidence Ordinance (Cap. 8), S. 26A of the Inland Revenue Ordinance (Cap. 112) and S. 19 of the Business Registration Ordinance (Cap. 310), as follows –

"any device for storing, processing or retrieving information".

3.3 The Electronic Transactions Ordinance (Cap. 553) does not attempt to define the terms "computer" or "computer system". Rather, it uses the concept of "information system", defined as follows –

"a system which –

(a) processes information;

(b) records information;

(c) can be used to cause information to be recorded, stored or otherwise processed in other information systems (wherever situated); and

(d) can be used to retrieve information, whether the information is recorded or stored in the system itself or in other information systems (wherever situated)".

Examples in other jurisdictions

3.4 In the Council of Europe's draft Convention on Cyber-crime (please see para. 14.2, Chapter XIV), a "computer system" means "*any device or a group of inter-connected devices which pursuant to a program performs automatic processing of data*".

3.5 The US Code Title 18 Section 1030 on "fraud and related activity in connection with computers" defines "computer" as follows –

"an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device"

3.6 The Canadian Criminal Code Part IX on "Offences Against Rights of Property – Offences Resembling Theft" provides the following definitions of "computer system" and "computer program" –

"computer system means a device that, or a group of interconnected or related devices one or more of which,

(a) contains computer programs or other data; and

(b) pursuant to computer programs,

(i) performs logic and control; and

(ii) may perform any other function,

computer program means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function."

Consideration

3.7 In a narrow sense, the term "computer" commonly conjures up the image of a stand-alone machine complete with a monitor, a keyboard and a central processing unit. However, in a broader sense, and with the development of the Internet and devices such as electronic personal data assistants and technologies such as Wireless Application Protocol, the term is increasingly taken to refer to a whole host of other items such as networked computer systems and many mobile electronic communication devices.

3.8 There are two sides to the argument of whether a clear legal definition of the term "computer" is required. On the one hand, technology is constantly evolving. What used to be understood as a stand-alone desktop machine or a huge mainframe system only a decade ago now denotes much more varied devices. A legal definition may therefore run the risk of either being too general or having to be updated frequently. On the other hand, leaving the matter entirely to the interpretation of the court may lead to widely different judgements depending on the inclination of the judges in question.

3.9 On balance, the Working Group sees merit in setting out in our law some parameters within which the concept of "computer" should be interpreted. The definition should not be unnecessarily restrictive lest it fails to cover new devices or technologies. It should be wide enough to cover such different items as stand-alone computers, computer systems and mobile telecommunication/information devices. As the term "computer" could be too narrow for present day circumstances, we are in favour of a more embracing term than "computer" to establish the legal parameters. The Working Group ***recommends*** that the term "information system" as defined in the Electronic Transactions Ordinance (Cap. 553) (para. 3.3 above) be used in place of "computer". We understand that the definition of "information system" has been drawn up having regard to the latest international developments in the field of information

technology. It was scrutinized by our legislature in the context of the Electronic Transactions Bill only fairly recently. (The Bill was passed in January 2000.) In addition, we understand that the Information Technology and Broadcasting Bureau will keep the Ordinance under regular review to take into account relevant developments. By linking the definition of "information system" to that used in Cap. 553, any future revisions to the latter will automatically apply to the former.

3.10 We have trawled through our laws and have identified a total of 76 sections in 35 ordinances where the term "computer" appears. (A complete list of these sections is at **Annex 3**.) A quick review of these sections indicates that they should be able to accommodate a change of terminology from "computer" to "information system". In principle, for greater consistency of our laws, we should align the terminology used in all the relevant sections. However, we recognize that there is the possibility that there are policy considerations that we are not aware of associated with the use of the term "computer" in particular sections. We would therefore ***suggest*** that the relevant Government bureaux should first be asked to consider those sections under their purview. Subject to their agreement regarding those sections under their purview, we ***recommend*** that the term "computer" in our legislation should be changed to "information system".

Shorthand expressions

3.11 Strictly speaking, there is no "hacking" offence in law. Rather, it is rendered as either "unauthorized access to computer by telecommunication" or "access to computer with criminal or dishonest intent". Similarly, the recommendations in paras. 3.9 and 3.10 are made with a view to facilitating understanding of the concepts of "computer" and "computer system" in the legal context, where much more precision is required than in everyday life. For ease of reference, the terms "computer" and "computer system" will continue to be used as shorthand expressions in the rest of this Report. Their meaning should however be construed as "information system" as defined in the Electronic Transactions Ordinance.

Chapter IV

Jurisdiction

Introduction

4.1 Computer crimes respect no territorial borders. This cross-border nature requires a new perspective to approach the traditional concept of jurisdiction. We examine the issues involved below.

Present position

4.2 In the physical world, the perpetrator of a crime is usually at or near the scene of the crime. Traditionally, therefore, the concept of jurisdiction is closely associated with geographical boundaries. Unless otherwise specified, the jurisdiction of the court is limited to acts done within the geographical boundaries of a country or territory. Generally, the common law regards an offence as being committed where the last act or event necessary for its completion took place, and jurisdiction is afforded where the offence is committed.

4.3 With the advent of communications has come cross-border crime. A partial response to the problem is mutual legal assistance agreements. These are bilateral agreements with other jurisdictions in criminal matters. They seek to ensure reciprocity between the contracting parties and enhance international cooperation in the fight against transborder crime. The major items of assistance covered by mutual legal assistance agreements typically include –

- identifying and locating suspects and witnesses;
- serving documents;
- obtaining evidence;
- executing requests for search and seizure;
- providing documentary evidence relevant to criminal matters;

- transferring of persons to give evidence or assisting confiscation; and
- tracing, restraining and confiscating property used or derived from crime.

4.4 Mutual legal assistance facilitates the collection of evidence of transborder crime, and should be useful in tackling cross-border cyber crime to some extent. However, in itself it does not solve the jurisdictional problem where transactions and events related to a crime take place in more than one jurisdiction.

4.5 Hong Kong enacted the Criminal Jurisdiction Ordinance (Cap. 461) in December 1994. The Ordinance is aimed at addressing the jurisdictional problems associated with international fraud. It gives the courts in Hong Kong jurisdiction over offences of fraud and dishonesty, as follows.

(a) Hong Kong courts will have jurisdiction if any of the conduct (including an omission) or part of the results that are required to be proved for conviction of the offence takes place in Hong Kong.

(b) An attempt to commit the offence in Hong Kong is triable in Hong Kong whether or not the attempt was made in Hong Kong or elsewhere and irrespective of whether it had an effect in Hong Kong.

(c) An attempt or incitement in Hong Kong to commit the offence elsewhere is triable in Hong Kong.

(d) A conspiracy to commit in Hong Kong the offence is triable in Hong Kong wherever the conspiracy is formed and whether or not anything is done in Hong Kong to further or advance the conspiracy.

(e) A conspiracy in Hong Kong to do elsewhere that which if done in Hong Kong would constitute an offence is triable in Hong Kong

provided that the intended conduct was an offence in the jurisdiction where the object was intended to be carried out.

The list of offences to which the Ordinance applies may be amended by an order of the Chief Executive in Council, but no order should be made without a draft having been approved by the Legislative Council. Of the offences created by the Computer Crimes Ordinance (please see para. 2.2 of Chapter II), the Criminal Jurisdiction Ordinance only covers false accounting done through the computer.

4.6 It is clear that many computer offences not covered by the Criminal Jurisdiction Ordinance may also be transborder in nature, for example, hacking; criminal damage through altering or erasing computer programs or data; Internet gambling etc. The problem of jurisdiction has to be addressed in earnest.

Legislation in other jurisdictions

4.7 The jurisdictional problem associated with computer crime was recognized in the United Kingdom at a fairly early stage. The UK Computer Misuse Act 1990 provides that UK courts have jurisdiction over offences covered by the Act if either the victim or perpetrator of the crime is in the UK. The offences covered include unauthorized access to computer program or data, unauthorized access with intent to commit or facilitate the commission of a further offence(5) and unauthorized modification of any computer content.

4.8 Similarly, the Computer Misuse Act of Singapore allows the prosecution of an offender for computer related offences committed within or outside Singapore. Where an offence covered by the Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore. The Act shall apply if, for the offence in question,

(5) Further offences are those for which a person of 21 years or above may be sentenced to imprisonment of five years or more.

- the accused was in Singapore at the material time; or
- the computer, program or data was in Singapore at the material time.

The offences covered by the Singapore Computer Misuse Act are – unauthorized access to computer material, access with intent to commit or facilitate commission of offence[6], unauthorized modification of computer material, unauthorized use or interception of computer service, unauthorized obstruction of use of computer and unauthorized disclosure of access code.

4.9 The draft Convention on Cybercrime published in April 2000 by the Council of Europe (please see para. 14.2, Chapter XIV) appeals to member states to establish jurisdiction over computer related offences when they are committed within their territory or on a ship, an aircraft or a satellite flying their flags or registered in them, or when they are committed by one of their nationals outside the territorial jurisdiction of any state.

Consideration

4.10 As cross-border crime, whether computer related or not, increases, current jurisdictional rules may present an unnecessary straitjacket. We have considered if the offences under the purview of the Criminal Jurisdiction Ordinance should be fundamentally changed. Instead of the present approach of listing each offence to be covered by the Ordinance, would it be simpler to adopt a generic description of "all offences triable on indictment", for example? That would obviate the need to identify each and every offence to which normal jurisdictional rules should not apply. However, this approach would change the basic principle regarding jurisdictional rules. The Criminal Jurisdiction Ordinance is meant to provide exceptions to the norm. Changing the ambit of the

(6) Offences covered are those involving property, fraud, dishonesty or causing bodily harm and which are punishable on conviction with imprisonment of not less than two years.

Ordinance fundamentally to cover in effect almost all criminal offences should not be attempted lightly and is beyond the Working Group' s remit. The question of jurisdiction is a major one involving complicated legal concepts. It requires careful and detailed examination of established legal principles and evolving case law, backed by considerable legal research and analysis. A comprehensive rather than compartmentalized approach is needed in order to ensure consistency. The Working Group therefore ***recommends*** that consideration be given to conducting a thorough in-depth study of the subject of jurisdictional rules in general to take account of the greatly increased ease of transportation and communications. This may well be a suitable assignment to be undertaken by, for example, the Law Reform Commission.

4.11 The in-depth review recommended in para. 4.10 above will necessarily take some time given the complex legal issues involved. The Working Group believes that more immediate relief is required where computer crime is concerned. We need to ensure that computer criminals will be brought to justice and will not be able to exploit the present loopholes. We consider how best to bring this about below.

4.12 One option would be to identify all offences which may be committed via the computer or the Internet and include them within the scope of the Criminal Jurisdiction Ordinance. However, the number of such offences could be very large. In addition, this approach could result in different jurisdictional rules applying to offences essentially similar in substance and different only with regard to whether the use of the computer or the Internet is involved. For instance, the situation might arise where one set of jurisdictional rules might apply to gambling offences in general and another set to Internet gambling.

4.13 Para. 4.12 above reinforces our belief that the whole question of jurisdiction should be addressed in a holistic fashion. For the time being, we consider that we should try to build on existing provisions as far as possible.

4.14 Our preferred option is to use S. 161(1)(a) of the Crimes Ordinance as a starting point. That section provides that a person who obtains access to a computer with intent to commit an offence commits an offence. This latter offence is similar in concept to the further offence approach in both the UK and Singapore. The key difference is with regard to the jurisdictional question – in both the UK and Singapore, the offence is covered by extended jurisdictional rules (please see paras. 4.7 and 4.8); in Hong Kong, it is not.

4.15 It would only be natural as well as much simpler and more direct to pursue the original offence if that was feasible. It is therefore not surprising that so far S. 161(1)(a) of the Crimes Ordinance has not been resorted to. However, if the jurisdiction is extended, the offence of accessing a computer to commit a further offence would be useful in catching criminal acts which would otherwise be impossible to catch. For example, a person outside Hong Kong using e-mails to threaten a person in Hong Kong with injury to that person, his reputation or property could be put under the jurisdiction of Hong Kong courts. As a first step, therefore, we ***recommend*** that the current offence of accessing a computer with intent to commit an offence (S. 161(1)(a) of the Crimes Ordinance) be brought under the coverage of the Criminal Jurisdiction Ordinance. In other words, Hong Kong courts should have jurisdiction over the offence if the person who obtains access to the computer for committing the offence is in Hong Kong or if the computer to which access is obtained for committing the offence is in Hong Kong.

4.16 The current penalty for accessing a computer with the intent to commit an offence is five years' imprisonment. We fully recognize that the act being punished is not the offence to be committed itself. However, we consider that, to be an effective deterrent, the penalty for an act done with a view to committing a certain offence should have regard to the severity of the offence to be committed. If the offence to be committed carries a penalty of, say, life imprisonment, it would appear that the act done with the intent to commit the offence should not be limited to only five years' imprisonment. We therefore ***recommend*** that the penalty for accessing a computer with the intent to commit an offence should be amended, to the

effect that it should be decided having regard to the severity of the offence to be committed. Of course, the penalty should not exceed the maximum penalty for the offence to be committed. Since the same consideration does not apply to other parts of S. 161(1) of the Crimes Ordinance, consideration may be given to creating a separate offence for the purpose and amending S. 161(1) accordingly.

4.17 We have considered whether there are offences other than accessing a computer with intent to commit an offence that should be put under the coverage of the Criminal Jurisdiction Ordinance. Given the considerations in paras. 4.10 and 4.12 above, we do not propose to substantially expand the coverage of the Ordinance at this stage. However, we ***recommend*** that the following offences, as modified to take into account the recommendations of this Report, should also be covered by the Ordinance –

- unauthorized access to computer by telecommunication (S. 27A, Telecommunications Ordinance); and

- other parts of the offence of access to computer with criminal or dishonest intent not covered by para. 4.15 above, i.e., with a dishonest intent to deceive, with a view to dishonest gain for oneself or another, or with a dishonest intent to cause loss to another (S. 161(1) (b), (c) and (d), Crimes Ordinance).

These offences may be said to be "pure" or "direct" computer crimes, in the sense that the computer is the main subject of, and not merely incidental to, the offences. It would be reasonable to apply the provisions of the Criminal Jurisdiction Ordinance to them pending an overall review of jurisdictional rules in general.

Chapter V

Encryption

Introduction

5.1 Encryption technology has developed very rapidly and has become increasingly popular. As a safety feature, encryption plays a useful role in protecting confidential or personal information. It is an important key to confidence in e-commerce, for example. However, criminals may also use encryption to protect their computer records and e-mail communications. Without the right decryption keys it will be very difficult, if not impossible, to detect the protected transactions and extract admissible evidence for prosecution. We examine the issues involved below.

Present position

5.2 The possibility of computer records required for evidence or investigation being encrypted is not always provided for in Hong Kong laws where computer records feature. Where it is, the legal requirement is usually for computer information "to be produced in a visible and legible form which can be taken away". **Annex 4** lists the relevant legislative provisions in this regard.

5.3 The existing formulation for computer information to be produced in a visible and legible form has not been fully tested. Nonetheless, there is doubt as to whether it may solve the encryption problem satisfactorily. None of the current provisions in this regard specifically refers to the need for ***decrypted*** information or plain text. It might therefore be argued that the present requirement for visible and legible information could be fulfilled by producing a print-out of codes and symbols. The latter, of course, would be of little assistance for either investigation or prosecution.

Examples in other jurisdictions

5.4 The following measures have been considered or adopted by other jurisdictions to address the encryption key problem –

- prohibiting unauthorized encryption;
- creating an offence for use of encryption in furtherance of commission of a criminal offence, concealing a criminal misconduct or obstructing government investigation of a criminal offence;
- providing for mandatory key escrow; and
- creating the power to require production of encryption keys by warrant or order.

We look at some selected examples below.

5.5 The Mainland of China, Russia and Saudi Arabia all prohibit the use of unauthorized encryption products.

5.6 The crypto policy paper of Sweden published in May 1999 argues that the voluntary deposit of private encryption keys in escrow, with legal access, is a solution for balancing law enforcement and user needs.

5.7 In the US, the Draft Key Recovery Legislation of 1998, the E-Privacy Act of 1998, the Security and Freedom through Encryption Act (SAFE) of 1999 and the Promote Reliable On-line Transaction to Encourage Commerce and Trade (PROTECT) Act of 1999 all put forward provisions which would criminalize the use of encryption in furtherance of the commission of a criminal offence or in covering up a crime. To our knowledge, none of these provisions has been enacted yet.

5.8 In Singapore, under the Misuse of Computer Act, a police officer authorized in writing by the Commissioner of Police may access any information, code or technology which has the capability of re-transforming or unscrambling encrypted data into a readable and comprehensible format.

5.9 In Malaysia, the Digital Signature Act allows a police officer conducting search under a search warrant to be given access to computerized data and be provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of the computerized data.

5.10 In the United Kingdom, the recently passed Regulation of Investigatory Powers Act 2000 enables authorized persons to serve written notices requiring the surrender of protected data in plain text or the keys to unlock the data. The power to serve such notices would be conferred by a Secretary of State or a judge depending on the nature of the information in question.

5.11 Both the Netherlands and Belgium have prepared bills which would require third parties to release encryption keys but would not compel a person to incriminate himself.

Consideration

(a) Need for change

5.12 It may be argued that it is part and parcel of an investigator's duty to make sense of the evidence that he has gathered. There are many commercially available decryption programs. There are also programs specially developed by investigators themselves to decipher encrypted data. Thus one possibility is to continue to rely on these means.

5.13 However, given the large number of encryption programs and the even greater number of encryption possibilities, breaking encrypted codes is increasingly difficult. More importantly, the concern here is producing admissible evidence from encrypted data in legal proceedings, and not decoding information for intelligence purpose. In the former case, it is necessary to prove beyond reasonable doubt that the decryption program or method used was the right one and that the decrypted data is indeed the correct data.

5.14 Some have suggested that the problem should be tackled at source, i.e., by regulating the use of encryption methods in the first place. In our view, the effectiveness of such regulation on its own is likely to be limited. It does not give investigators access to the decryption keys where they have indeed been used. Similarly, criminals are unlikely to deposit their keys in an escrow account. More importantly, encryption may be used for perfectly legitimate purposes, and blanket regulation of its use might be an overkill in a free market economy. We consider that it would be more appropriate and direct to enable law enforcement agencies to be provided with the decryption tool or the decrypted text (including all the images and sounds) ***when necessary and justified***. We ***recommend*** that legislation be introduced for the purpose.

(b) Options

5.15 Purely from the point of view of enforcement facilitation, it would be desirable if the law enforcement agency involved in an investigation could have fairly uninhibited access to the decryption key or decrypted text. In most cases, the relevant computer records would already be in the possession of the agency. It would only be a matter of deciphering the codes. A delay in getting hold of the decryption key or decrypted text could result in missing golden opportunities of, say, arresting accomplices or seizing crime proceeds.

5.16 At the same time, we should not lose sight of the need for safeguards against possible abuse of the power to demand disclosure. We have therefore examined several possible options on the basis of the examples of other jurisdictions set out in paras. 5.5 to 5.11 above.

5.17 The first option envisages entrusting the power to compel the provision of the decryption key or decrypted text to a sufficiently senior officer of the law enforcement agency involved. For example, it could be stipulated that only officers personally authorized, in writing, by the head of the respective enforcement agency could have such powers. Additionally, the authorization should be case specific. The second option is a variant of the first, by giving the power to a Bureau Secretary, for example, the Secretary for Security for offences under the Crimes Ordinance and the Secretary for Commerce and Industry under the

Copyright Ordinance. The third option envisages the bringing in of judicial scrutiny. This would strengthen the checks and balances available institutionally to ensure that the power to demand the decryption key or decrypted text would not be used lightly.

5.18 The first two options would presumably be faster. This would be useful in the context of investigating computer crime where speed is of the essence. Giving the power to the head of the enforcement agency or to the Bureau Secretary concerned would ensure that the power would not be used indiscriminately. Rationally, either option could suffice. However, we realize that any compulsion to disclose information, especially where the disclosure may incriminate oneself, should be treated most seriously. The right of an individual to not incriminating himself, privacy and confidentiality of information should be respected as far as possible. Entrusting the power to demand compulsory disclosure to a non-executive body would enhance perceptions of sufficient checks and balances. On balance, therefore, the Working Group ***recommends*** that some form of judicial scrutiny should be introduced for the disclosure requirement.

(c) "Production orders" process

5.19 In framing the judicial scrutiny procedures, we have drawn reference from the provisions of the Organized and Serious Crimes Ordinance (Cap. 455) regarding what are commonly referred to as "production orders". Under section 4 of the Ordinance, the Secretary for Justice or an authorized officer may make an ex-parte application to the Court of First Instance for an order for materials relevant to an investigation into an organized crime or an offence related to an organized crime to be produced or given access to. The court has to be satisfied that a number of conditions are met before granting the order. For example, where the investigation is into an organized crime, the court has to be satisfied that there are reasonable grounds for –

(a) suspecting that the organized crime has been committed;

(b) believing that the material to which the application relates is likely to be relevant to the investigation and does not include items subject to legal privilege; and

(c) believing that it is in the public interest for the materials to be produced or given access to.

5.20 A person subject to a "production order" may apply to the court for the discharge or variation of the order. However, he cannot be excused from the order because the material might incriminate him. Any person who fails to comply with the order commits an offence and is liable to a fine of up to $100,000 and imprisonment for one year.

5.21 In practice, an application for a "production order" is made by either the Secretary for Justice or an authorized officer only after close scrutiny by the Secretary for Justice. In a case with very strong evidence, the investigator will seek advice from the Secretary for Justice on the preparation of the affidavit before he makes the application to the Court of First Instance. In a borderline or complex case, the application will be made by the Secretary for Justice. Coupled with judicial scrutiny, there are sufficient safeguards in ensuring that an application is only made and granted where necessary and justified.

5.22 The Working Group ***recommends*** that a process similar to that for applying for "production orders" under section 4 of Cap. 455 be adopted for orders to allow access to encoded computer information relevant to an investigation. The access may be provided in the form of the plain or decrypted text or the necessary passwords, encryption codes, decryption codes, software, hardware and any other means to enable comprehension of the computer information in question.

5.23 As regards the scope of the proposed legislation, there are several possibilities. First, we could apply it to organized and serious crimes which are already covered by the production order requirement under the Organized and Serious Crimes Ordinance (Cap. 455). However, this would cover only offences related to activities of a triad society or offences committed by two or more persons involving substantial planning and organization. This scope is too limited for our purpose.

5.24 Another possibility is to apply the disclosure requirement to all instances where encrypted computer information may be seized or otherwise obtained in connection with a criminal investigation. This general approach would be easier to implement, and would ensure consistency in treatment. The potential downside is that this might cast too wide a net. It might be argued, for example, that some "petty" computer crime does not warrant the compulsion to disclose the decryption key, which should only be reserved for more serious offences. Given the severity of the measure, which could involve requiring the disclosure of self-incriminating evidence, we are sympathetic to this view.

5.25 To cater for the above considerations, we ***recommend*** that an extra safeguard be built in by limiting the disclosure power to offences of a more serious nature. Only offences attracting a maximum penalty on conviction of not less than, say, 2 years' imprisonment should be subject to this disclosure requirement.

5.26 Subject to acceptance of the recommendations in paras. 5.22 and 5.25, we further ***recommend*** that there be suitable legal protection of the confidentiality of the information obtained through the disclosure procedures. It should also be stipulated that evidence obtained as a result of compulsory disclosure should be admissible in court.

5.27 It is critical that the proposed legislation has teeth. Substantial financial stakes could be involved. There should therefore be penalties sufficiently severe to deal with the failure, without reasonable excuse, to comply with an order to allow access to encrypted information. A mere fine would not be a sufficient deterrent, as it could be treated just as an operating cost. We ***recommend*** that the penalties should in principle be commensurate with those for the specific offence under investigation.

Chapter VI

Protection of Computer Data

Introduction

6.1 In this chapter, we examine how development of the computer and the Internet has accentuated the problem of data protection, and evaluate the need for increased protection for computer data against unauthorized access and use.

Present position

6.2 At present, only the Personal Data (Privacy) Ordinance provides a legal definition of the term "data". Section 2 of the Ordinance defines "data" as "*any representation of information (including an expression of opinion) in any document, and includes a personal identifier.*" Thus defined, data has a very wide meaning, and includes, for example, copyright works, personal data, credit card details, trade secrets, passwords etc.

6.3 Currently, some well-defined types of data, such as copyright works, personal data and insider information for securities trading are covered by specific legislation. However, data as a whole is not protected by statute. Violations of rights arising from data not specifically protected by statute are dealt with differently. For example, where there is a breach of commercially sensitive information communicated in confidence, civil suits may be resorted to. Where credit card information is stolen for shopping fraud, it is normally dealt with as fraud or the physical theft of the credit card itself, and hence the question of "stolen" information is side-stepped.

6.4 The need to protect computer data was recognized as early as 1993, with the enactment of the Computer Crimes Ordinance. For example, with the extended meaning of "property", the offence of criminal damage to property under the Crimes Ordinance (Cap. 200) now covers the misuse

of computer data (through altering, erasing or adding any data to the contents of a computer). The amended offence of "burglary" in the Theft Ordinance (Cap. 210) also covers entry into a building with intent to unlawfully alter, erase or add any computer data. In addition, it is an offence, under the Telecommunications Ordinance (Cap. 106), to cause, by telecommunication, a computer to perform any function to obtain unauthorized access to any data held in a computer.

6.5 Nonetheless, under present legislation, the "theft" of computer data itself is not a criminal offence. There is also no sanction against the receiving, handling or copying of computer data obtained without authorization.

Legislation in other jurisdictions

6.6 Legislation in other jurisdictions to protect computer data mainly takes the form of protecting computer data against unauthorized access. The data protected may be general or specific. In the latter case, computer passwords are the main target of protection. Paras. 6.7 to 6.13 set out some examples.

6.7 In the UK, under the Computer Misuse Act, it is an offence to cause a computer to perform any function with intent to secure unauthorized access to any data held in any computer.

6.8 In the US, federal legislation US Code Title 18 Section 1030(a)(b) creates an offence for knowingly and with intent to defraud traffics in any password or similar information through which a computer may be accessed without authorization.

6.9 Under the Canadian Criminal Code, it is an offence for anyone to, fraudulently and without authorization, obtain any computer service; intercept any function of a computer system; and use a computer system to commit an offence of mischief in relation to data or a computer program.

6.10 In Germany, the offence of "data espionage" applies to any person who obtains without authorization data which is not meant for him and which is specially protected against unauthorized access. The offence is expressly limited to data which is stored or transmitted electronically or magnetically or in any form not directly visible.

6.11 Under Malaysia's Computer Crime Act 1997, it is an offence for a person to communicate directly or indirectly a number, code, password or other means of access to a computer to any person other than a person to whom he is duly authorized to communicate.

6.12 In Singapore, under the Computer Misuse Act, unauthorized access to computer material is an offence. In addition, the Act prohibits the unauthorized disclosure of passwords or access codes for gaining access to any computer program or data for any wrongful gain, unlawful purpose, or for causing wrongful loss to others.

6.13 The draft Convention on Cybercrime published by the Council of Europe in April 2000 (please see para. 14.2, Chapter XIV) appeals to member states to offer protection against computer passwords or codes which are intended to be used for accessing a computer system without authority.

Consideration

(a) Need for protection

6.14 The problem of data protection is not unique to the cyber environment. For example, credit card information may be stolen through a physical theft of the card concerned, and not necessarily through unauthorized tapping into a credit card data bank or breaking into an Internet purchase transaction. However, the development of the computer and the Internet accentuates the problem in several respects, as follows.

(a) The volume and speed of virtual data transactions have increased significantly.

(b) The risk of massive data being accessed and copied for subsequent unauthorized use has increased considerably. The scale involved may also be huge. Entire data banks may be copied or otherwise tampered with in seconds, which is unlikely to be the case with physical data.

(c) The "loss" may not be immediately apparent. Often the victims may only find out, if at all, after some delay. The physical loss of, say, a credit card, on the other hand, will be noticed much more easily.

(d) The ability to fall back on traditional legal remedies is increasingly limited. For example, in the cyber world, credit card details are "stolen" without the credit card itself being taken away. While physically stealing a credit card may be caught by the existing offence of "theft", unauthorized access to credit card details through the Internet may not.

6.15 The potential financial loss through unauthorized access to data in the cyber world could be enormous. The potential damage to consumer confidence and hence the further development of e-commerce is also considerable. **Annex 5** gives a few examples in this regard. Although data protection is not a concern peculiar to the cyber world, therefore, there is a strong case for ensuring that data stored on or transmitted through the computer and the Internet are adequately protected.

(b) Options

6.16 We have considered the possibility of treating computer data as property which may be stolen. This would involve amending the current definition of the term "property" in the Theft Ordinance (Cap. 210)[7] to include computer data. The definition of the term in the Crimes Ordinance (Cap. 200) in this regard would provide a good starting

(7) The current definition of "property" in Cap. 210 is "money and all other property, real and personal, including things in action and other intangible property".

point —"any program, or data, held in a computer or in a computer storage medium, whether or not the program or data is property of a tangible nature". This arrangement would appear to be a relatively straightforward one as there is a ready piece of legislation in place. An amendment to the definition of the term "property" in the Theft Ordinance would make the other provisions of the Ordinance applicable to the theft of computer data. The amendment would also bring the definition of the term "property" in the Ordinance in line with that in the Crimes Ordinance.

6.17 On closer examination, however, the approach in para. 6.16 is not problem-free. The difficulty relates to the very concept of "theft". Under the Theft Ordinance (Cap. 210), a person commits theft if he dishonestly appropriates property belonging to another "with the intention of permanently depriving the other of it". It is obvious that there would be difficulty in applying this concept to computer data "theft" without adaptation. This is because the "theft" of data in the cyber environment invariably takes the form of unauthorized access to or copying of data, whether for subsequent use or not, and the question of permanent deprivation does not arise. In addition, questions of to whom computer data belongs and whether a dishonest intent must necessarily be present might be raised if the theft concept was to apply to computer data. On balance, we consider it more productive to see how to build on and add to computer data protection which is already in place (para. 6.4).

6.18 Our starting point is the existing offence of unauthorized access to computer data by telecommunication under the Telecommunications Ordinance. We note that the concept of unauthorized access is clearly set out in S.27A of the Ordinance –

"access of any kind by a person to any program or data held in a computer is unauthorized if he is not entitled to control access of the kind in question to the program or data held in the computer and— (i) he has not been authorized to obtain access of the kind in question to the program or data held in the computer by any person who is so entitled; (ii) he does not believe that he has been so authorized; and (iii) he does

not believe that he would have been so authorized if he had applied for the appropriate authority."

As long as the unauthorized access is done by telecommunication, criminal or dishonest intent does not have to be proved. Next, it is an offence under S. 161 of the Crimes Ordinance to access a computer, with or without authority, with a view to dishonest gain for oneself or another, or with a dishonest intent to cause loss to another. The means of access is not specified and should therefore include any means. In addition, under S. 60 of the Crimes Ordinance, the misuse of a computer, including altering, erasing or adding any data in the computer, constitutes criminal damage to property if done without lawful excuse or recklessly.

6.19 We consider that, taken together, the above provisions already cover much of what needs to be protected. We ***recommend*** the following improvements.

(a) In terms of coverage, it is clear that the current provisions already cover all data held ***in*** a computer. For the avoidance of doubt, they should be clarified to include all data transmitted or being transmitted via a computer or the Internet. This would cover unauthorized interceptions, for example. The idea is to catch all computer data at all stages of storage or transmission. This would also obviate the need to define each and every type of data that requires protection (e.g., credit card details).

(b) For the avoidance of doubt, the term "access to computer" should be clarified to include access to a computer[(8)] as well as the programs and data stored therein.

(c) Currently S.27A of the Telecommunications Ordinance limits the offence of unauthorized access to that achieved by means of telecommunication. This is unnecessarily restrictive. Unauthorized access by any means, e.g., through a "stolen"

(8) See Chapter III on definition of the term "computer".

password with or without the use of telecommunication, should also be made unlawful. If this widening of scope is accepted, we will need to consider whether the Telecommunications Ordinance continues to be the most appropriate vehicle for the offence. This should be addressed at the stage of law drafting.

(d) Receiving, retaining and handling/trafficking of computer data known to have been obtained through unauthorized access to the computer should be prohibited. This would plug the current loophole where a third party could in theory buy "stolen" computer data without committing an offence.

(e) It should also be illegal to sell, distribute and make available any computer password or access code for unlawful purposes. This would deal with situations of, for example, a disgruntled or dishonest employee making available passwords that he had come to know in the course of his duties to unauthorized persons, or a "dealer" who collected such passwords from various sources for on-selling to others for unlawful purposes. Since there are numerous occasions when passwords are distributed for perfectly legitimate purposes, the offence must be accompanied with the knowledge that –

- the disclosure is being made without authority; and
- the passwords would be used for wrongful gain for oneself or another, an unlawful purpose or causing wrongful loss to another.

In addition, the meaning of passwords, access codes and similar terms should be clearly defined to refer to information that may be applied directly and without further processing for assessing a computer. This would avoid casting too wide a net by catching programs or other information that may indirectly lead to unauthorized access to the computer after detailed manipulation. (We deal with the question of so-called "hacking tools" in para. 6.23 below.)

6.20 Unlawful access to the computer and the programs and data therein may result in significant losses. We have therefore already pointed out in para. 2.7, Chapter II, that a custodial term is required as penalty for the hacking offence currently covered by S. 27A of the Telecommunications Ordinance. A question that may arise is whether a custodial term is warranted if the unauthorized access is made to merely satisfy curiosity or "just for fun". Would education or a token fine suffice?

6.21 We certainly agree that more should be done on the education front to discourage computer users, in particular the younger generation, from accessing others' computer systems and data without authority. (Please see Chapter X on the role of education in preventing computer crime.) At the same time, we believe that we should not inadvertently create shields behind which perpetrators may hide, or give the wrong message that some kinds of hacking are not viewed seriously. At the very least, unauthorized access to computer programs or computer data is a violation of the right to keep one's information private and confidential. The act is rarely accidental, as it almost invariably involves the intentional tampering of security measures. The analogy is therefore not accidentally opening an unlocked door, but intentionally breaking into locked and guarded premises. In addition, regardless of the hacker's intention, it would be very difficult to guarantee that the programs and data accessed without authority are completely contamination free. They may well be infected with the hacker's computer viruses, for example. By eroding user confidence, hacking hinders the development of e-commerce.

6.22 The possible serious consequences of unauthorized access to computer data are sufficiently well known, and it would at least be reckless to intentionally ignore these consequences. As pointed out in para. 6.16 above, conceptually, the act may be seen as akin to theft. The offence of theft currently carries a maximum sentence of imprisonment for ten years upon conviction on indictment. Prima facie, a sufficient deterrent for the offence of unauthorized access to computer programs and data should not be less than that for theft. We therefore ***recommend*** that the

maximum penalty for the offence be increased accordingly. Of course, each case has to be considered on its own merits, and it is entirely within the powers of the court to impose a lesser sentence where justified.

(c) Hacking tools

6.23 The Working Group has considered the suggestion to outlaw the production, distribution, sale or use of hacking tools, i.e., programs which may enable unauthorized access to computer programs or data. We believe, however, that many so-called hacking tools may serve a legitimate purpose. For example, system managers may use these tools to test the vulnerability of their systems so as to fortify their security measures. It will be very difficult to tell when a hacking tool is solely for the unlawful purpose of hacking and when it may be used for education or other legitimate purposes. We therefore find it impracticable to legislate against hacking tools. We ***recommend*** that the proposal should not be pursued.

(d) Protection of data in general

6.24 In making the above recommendations, the Working Group has debated extensively whether we would inadvertently be creating an inconsistency between the treatment of computer data on the one hand and physical data on the other. We acknowledge that there could well be an anomaly if, for example, the trafficking of data obtained through unauthorized access to a computer was an offence while the trafficking of such data obtained through another means was not. After careful consideration, however, we believe that there are characteristics pertaining to computer data that may not necessarily apply on a similar scale to data kept in another medium (please see para. 6.14). To our knowledge, legislation in other jurisdictions seeking to protect computer data does not normally extend to non-computer data either. This has also been the approach adopted in the current offence of unauthorized access under the Telecommunications Ordinance.

6.25 From the Working Group's perspective, computer data protection deserves priority attention. Our recommendations have been made accordingly. Whether and how the subject of data protection in general should be tackled is beyond the remit of the Working Group. We would nonetheless wish to point out that it will be necessary for any possible anomalous situation to be studied and rectified as appropriate.

Chapter VII

"Deception" of Computers

Introduction

7.1 It is a common law tenet that a machine cannot be deceived. Given that computers are also machines, we need to examine the implications of this tenet on computer crime.

Present position

7.2 Legally, a machine, which includes a computer, cannot be deceived. Offences of deception require the deception of a human being. However, nowadays computers do "make decisions" by, for example, accepting on-line shopping orders according to a pre-set program. The common law tenet therefore calls into question whether it would be possible to secure successful prosecutions against people who provide false information, including stolen passwords and credit card details, to obtain goods, services and credit from victims via the Internet. The matter has not yet been tested in Hong Kong courts.

7.3 Effecting deception by computers is covered by the present offence of access to the computer with criminal or dishonest intent under S. 161 of the Crimes Ordinance (Cap. 200). S. 161(1) reads –

> *"Any person who obtains access to a computer –*
>
> *(a) with intent to commit an offence;*
>
> *(b) with a dishonest intent to deceive;*
>
> *(c) with a view to dishonest gain for himself or another; or*
>
> *(d) with a dishonest intent to cause loss to another,*

whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years."

In practice, S.161(1)(b) has not been resorted to since its enactment. Rather, paragraphs (c) and (d) have been relied on to overcome the potential difficulty caused by the common law tenet. The offence will be completed once a person has accessed the computer for providing another party with false information to gain something for himself or another or cause loss to another. It is therefore not necessary to prove that the machine in question, i.e., the computer, has been deceived.

Examples in other jurisdictions

7.4 The United Kingdom Law Commission has on a number of occasions considered whether there is a need to fill the gap resulting from the requirement that a human being must be deceived in order to make out the offences of deception in its legislation on theft. The Commission's view has been that while there is a case for reform, the gap in the law is only a small one because the dishonest manipulation of machines almost always involves the commission of another offence, for example, theft, or making of a false instrument or false accounting. If a person uses a computer, and supplies some other person's credit card data with a view to obtaining property, then he commits the offence of theft. The cost of the item purchased will in due course be debited to the credit card owner's account. This debiting constitutes a theft of the chose in action between the credit card issuing institution and the customer. In its 1999 consultation paper on fraud and deception, the Commission is of the provisional view that the "tricking" of machines should be dealt with in the context of theft rather than deception.

7.5 As far as the Working Group is aware, only Alaska, USA, has explicitly ruled out the common law tenet as a defence by enacting the following provisions in the Alaska Statutes, Title 11 Criminal Law, Chapter 6, Offences Against Property –

"*In a prosecution under this chapter for an offence that requires 'deception' as an element, it is not a defence that the defendant deceived or attempted to deceive a machine. For purposes of this section, 'machine' includes a vending machine, computer, turnstile or automatic teller machine.*"

Consideration

7.6 As pointed out in para. 7.3, S.161(c) and (d) may be used to overcome the potential difficulty with the common law tenet that a machine cannot be deceived. We also note that S.161(1)(b) of the Crimes Ordinance has not been resorted to since the enactment of S. 161. As far as computer crime is concerned, therefore, the Working Group believes that the common law tenet has so far not posed significant difficulties.

7.7 Although S.161(1)(b) has not been used so far, we consider that it may still be useful. It may, for example, apply in cases where a computer is accessed for the purpose of deceiving a human being who has to process the information received via the computer, and where it is difficult to prove gain or loss. Given the common law tenet, however, this paragraph will not apply where the human being's intention is captured in a pre-set program as to how information received should be processed and where no human intervention is involved in such processing. The Working Group has therefore considered if the paragraph should be amended to provide that the target of deception may be either a human being or a machine.

7.8 On the one hand, with technological developments, computers may be programmed to perform many functions that used to be carried out by humans. Increasingly many decisions are "made" by computers. Conceptually, it may be argued that insofar as computers are capable of carrying out human commands, they should be capable of being "deceived" as well. It would therefore seem unnecessarily restrictive to stick to the tenet that only humans may be deceived.

7.9 On the other hand, given the construction of S. 161(1) of the Crimes Ordinance, any gap created by the common law tenet is a small one only. In practice, we have not come across any significant example of "deception" of computers that may not be dealt with by paragraphs (c) or (d) of the section. ***Insofar as computers are concerned***, therefore, the Working Group considers that current legislation is sufficient to cover the "tricking" of computers instead of human beings.

7.10 Nonetheless, if we move beyond computers, there is indeed a problem with the "deception" of machines where the advantage obtained is a service (as opposed to goods or property). For instance, if a person "tricks" a coin-operated shoe-polishing machine to polish his shoes without the rightful payment, he is not guilty of any offence. This is because there is no legislation similar to S. 161(1)(c) and (d) of the Crimes Ordinance governing machines in general. While recognizing that the matter falls outside our remit, the Working Group ***recommends*** that consideration be given to carefully studying and rectifying this gap. There are at least two possible approaches to the problem. One would involve solving the problem for all machines in a general way. For example, it might be deemed that machines were capable of being deceived, or it could be expressly stipulated that it would be no defence to argue that the target of deception was a machine. The other approach would involve identifying those machines the misuse or tricking of which should be specifically outlawed, as in the case of parking meters. We would suggest that this may be a good topic for consideration by a body such as the Law Reform Commission, for example, in the context of studying our law on deception and theft in general.

7.11 Our concern about consistency between deception in the cyber world and that in the physical world has also pointed to the necessity to review the adequacy of the present penalty for the deception and dishonest intent parts of the present offence of access to the computer with criminal or dishonest intent (S. 161(1)(b), (c) and (d) of the Crimes Ordinance). (The penalty for S. 161(1)(a) has been dealt with separately in Chapter IV.) The penalty is currently set at a maximum of five years' imprisonment. We note, however, that the deception related offences in

the Theft Ordinance attract a maximum sentence of 10 to 14 years of imprisonment. Given that deception via the computer or the Internet could cause damage no less severe than deception in the physical world, we ***recommend*** that, in principle, a maximum penalty no less than that for offences of a similar nature under the Theft Ordinance, i.e., a minimum of 10 years' imprisonment, should be put in place for the deception and dishonest intent parts of the present offence of access to the computer with criminal or dishonest intent. As pointed out in Chapter VI, it is entirely within the powers of the court to impose a lesser sentence within the maximum prescribed by law, but we should not create the wrong impression that deception via the computer is a lesser evil than that committed by other means.

Chapter VIII

Assistance from Internet Service Providers (ISPs)

Introduction

8.1 Much computer crime is conducted via the Internet. It would therefore be useful to examine whether and how Internet Service Providers (ISPs) should help in combating or preventing computer crime. We look into the relevant issues below.

Background

8.2 In the investigation of an offence that involves the use of the Internet, both accounting records and session records are useful. Accounting records provide information on the identity of the account holder. They include such details as the name of an account subscriber, his identity document particulars, his contact details and payment instructions. Session records, on the other hand, provide the trails to track an Internet transaction. They typically include such details as the log-in and log-out time, and the assigned Internet Protocol (IP) address (please see para. 8.3). In some cases, the address of the webpage or e-mail account accessed and the caller's number, where there is a caller number display function, may also be captured. Session records may therefore be used to trace an Internet transaction to a particular account subscriber and, where there is a caller identification function, to track that transaction to a specific location.

8.3 An important lead for tracing the perpetrator of a computer crime is the IP address assigned to his account. In a dial-up system, this address code is assigned by the ISP each time when a person logs on the ISP's system for access to the Internet. The address becomes available for reassignment when the person logs off the system. The only way of confirming to whom a particular IP address was assigned at any given time is to study the log records of the ISP if they are kept. Leased line accounts, however, are assigned fixed IP addresses.

Present position

8.4 There is currently no requirement for licensed ISPs (which numbered about 200 at the end of July 2000) to retain log records. Nonetheless, we understand that ISPs do keep log records of dial-up accounts for varying periods. According to an informal survey of selected ISPs by the Hong Kong Internet Service Providers Association, the length varies from one month to three years. In addition, major ISPs (who among themselves have over 80% of the total market share) tend to keep log records for six months or more. The log records are mainly kept for billing purpose. The period for which ISPs hold the log records depends largely on the capacity of their computer systems. Given that leased line accounts are charged a fixed fee irrespective of log-on time, ISPs do not keep log records of these accounts. The ISPs also keep varying details of subscribers for accounting purpose.

8.5 In addition to commercial ISPs, universities also provide Internet access, but the facility is limited to their staff and students. Although the service is free of charge, we understand that the university systems do maintain log records of the accounts for reasons of –

- security : to monitor unlawful access by outsiders;
- internal audit : to monitor possible abuse of system; and
- research and development : to identify priorities in the allocation of resources —more resources may be allocated to popular sites.

Concerns

8.6 The record-keeping practices vary from ISP to ISP. Some records may be destroyed soon after the billing purpose is fulfilled and may not be kept for long enough from the point of view of facilitating law enforcement. The amount of details kept also varies. In addition, globally, there is an emerging trend that ISPs will offer free Internet

access. With that, the need to keep log records for billing purpose will fall away. The enforcement agencies would naturally like to ensure that ISPs not only continue to keep sufficient session and account records, but also keep them for a minimum period of, say, 6 months. Apart from log records, they have suggested that the calling line number should also be kept. An indicative list of the types of records which computer crime investigators have suggested that ISPs should keep is at **Annex 6**.

8.7 Separately, some have suggested that ISPs may contribute more to combating or preventing computer crime through a speedy take-down of offending sites. There has also been a suggestion that ISPs prohibit multiple log-in to reduce the possibility of accounts being used without authorization. Another suggestion is to impose a credit limit on credit card payment transactions through the Internet, thereby limiting the damage of Internet shopping fraud.

Examples in other jurisdictions

8.8 In September 1999, the Data Protection Working Party (the Working Party) of the European Commission delivered its recommendations on the preservation of traffic data by ISPs for law enforcement purposes. Placing emphasis on the protection of personal data privacy, the Working Party examined the maximum period, instead of the minimum period, that ISPs should keep records of their clients. It recommended the European Commission to propose appropriate measures to harmonize the period for which telecommunication operators and Internet service providers are allowed to keep traffic data. The period should be as long as necessary to allow consumers to be able to challenge the billing but otherwise as short as possible in order not to overburden operators and service providers.

8.9 In April 2000, the Council of Europe released its first draft of a convention on cyber crime for public discussion (please see para. 14.2, Chapter XIV). The draft convention covers, among other things, the requirement for member states to adopt legislative or other measures to compel a person to preserve traffic data concerning a specific

communication for the purpose of criminal investigation. This requirement, if put into practice, would relate to a specific request and would not be a general requirement for ISPs to keep records.

8.10 The Report of the US President's Working Group on Unlawful Conduct on the Internet (USWG) released in March 2000 points out that some members of the Internet industry do not retain certain system data for a long enough period to permit law enforcement agencies to identify online offenders. However, the USWG does not support any mandatory data retention requirement. It proposes instead that the industry itself should evaluate the costs and benefits of data retention by taking into consideration market needs, protection of consumer privacy and public safety. The USWG advises the industry to give appropriate weight to the wider value to itself and to society of retaining certain information that may be essential to apprehending a lawbreaker.

8.11 The Group of Eight (G8) conference held in Paris in May 2000 discussed the proposal of mandatory requirements on ISPs to keep records on their subscribers. This however evoked strong objections from ISP representatives who claimed that any tight regulation could burden the industry with extra costs and stifle the growth of e-commerce.

8.12 As regards other forms of ISP cooperation, the US Digital Millenium Copyright Act enacted in 1998 sets out the notice and takedown procedures to be followed by online service providers (OSPs) against copyright infringing articles. A copyright owner may notify the relevant OSP if he believes that a site contains matters misusing his copyright. On receipt of such a notice or if the OSP independently becomes aware of the infringement, the OSP must expeditiously remove the material or disable public access to the site. If the OSP complies in good faith with the statutory requirements, the law immunizes it from liability to subscribers and third parties. If a subscriber files a proper "counter notice" attesting to his lawful use of the materials, the OSP must promptly notify the copyright owner and within 14 business days restore the materials, unless the matter has been referred to a court.

Consideration

(I) Record-keeping by ISPs

8.13 Traffic data and subscriber details are certainly important tools in investigating cyber crime. Although present record-keeping practices vary among ISPs, the latter do tend to keep both accounting records and session records for their own purposes. Our law enforcement agencies may obtain such records for investigation purposes according to the relevant provisions of the legislation governing their operation. Where necessary, an application to the court for search warrants will be made. Where the records contain personal data, exemption is granted by S. 58 of the Personal Data (Privacy) Ordinance (Cap. 486). So far, these agencies have not experienced insurmountable problems in accessing these records when necessary. Nonetheless, we have considered the need for and practicability of various proposals to strengthen the present arrangements.

(a) Subscriber details

8.14 At present ISPs may rely on different means to verify the personal details provided by a prospective subscriber. For example, the details of the subscriber's identity document may be noted down and some proof of address (in the form of, for example, utility bills) may be cross-checked. Nonetheless, in our informal discussions with some ISPs, it has been put to us that it would facilitate the verification of subscriber identity if ISPs are expressly required by law to retain photocopies of their clients' identity documents.

8.15 We understand that the Office of the Privacy Commissioner has issued the "*Code of Practice on Identity Card Number and other Personal Identifiers*". The code sets out the conditions when a copy of an identity card may be kept. We believe that code already provides guidance for ISPs, among others, to follow in handling personal data. In addition, where necessary and justified, the relevant details of a prospective client's identity card may be taken down at the point of inspection. It

therefore seems that the added value of a statutory requirement for ISPs to retain photocopies of their clients' identity cards on top of present arrangements is very small.

8.16 It might be argued that the proposed statutory requirement would curb instances where subscriber details are not checked vigorously because of the fear of losing a prospective client to one's competitor. However, to tackle the problem at source, it would be more effective for subscriber particulars to be checked carefully in the first instance. ISPs would risk not only their revenue and reputation but also the security of their systems and/or those of their clients if they do not insist on some basic good management practices. It does not seem a proportionate measure to legislate on the problem which may be solved by administrative means. We would ***recommend***, however, that law enforcement agencies should work out with representatives of ISPs an administrative guideline on the types of subscriber details that should be inspected at the point of opening an Internet account and those which should be kept for as long as the account is being maintained and for a reasonable period after the account is closed. This guideline should be compatible with the requirements of the Personal Data (Privacy) Ordinance.

(b) Caller's number

8.17 The Working Group has deliberated at length whether ISPs should be required by law to keep records indicating the caller's identification in respect of all transactions. In many computer crimes cases, the perpetrator uses a stolen account. Log records showing merely which account was assigned a particular IP address involved in a computer crime case may therefore not be particularly useful. Records showing the caller's number are however able to indicate the physical location from which an Internet message or command originated if the number involved belongs to a fixed telephone line. They are therefore valuable leads in investigating past events related to a computer crime.

8.18 On the other hand, the Working Group notes that the proposal is not without its problems. The first concern is cost. It is estimated that a caller identity display facility would cost about $25 per line per month[9], and an ISP could easily have hundreds, if not thousands, of lines. In addition, there would be extra storage cost for the data captured. The cost would likely have to be shouldered by the consumer ultimately. In informal discussions with us, some ISP representatives have pointed out that they have no need for caller numbers in running their business. If the requirement is imposed simply for law enforcement facilitation, then consideration should be given to the Government shouldering the cost. This argument cannot be accepted at its face value because, carried to the extreme, it could mean that the Government had to pay for all costs of compliance with legal requirements. We note that in some jurisdictions, for example, Australia and the United Kingdom, the approach has indeed been for the government to be given the power to specify minimum technical standards for communications carriers and service providers and to share part of the cost of compliance subject to conditions. This is however geared towards ensuring technical capability when certain investigative powers have to be resorted to, and not towards mandating the keeping of caller numbers on all transactions. To our knowledge, the latter is not a legal requirement in any developed economy.

8.19 A more important concern relates to the effectiveness of the proposal. The caller number display function may be disabled if the caller dials "133" when logging in. Consideration has also been given to requiring ISPs to refuse service to callers whose number cannot be captured. If the ISP's system is so programmed, however, there will be the following difficulties.

- The caller number display function enables the display of the telephone number of local calls only. Clients travelling abroad therefore cannot access ISP service by making long distance calls back to their ISPs in Hong Kong.

(9) This is the tariff, approved by the Telecommunications Authority, levied by the dominant fixed line telephone company.

- The caller number display function may not always enable the display of the caller's number from PABX calls. Clients calling from PABX systems may therefore not be able to access ISP service.

8.20 The Working Group has considered a similar proposal, which envisages fixed line telephone companies rather than ISPs keeping caller line identification (CLI) data. The CLI function can keep track of calls even if "133" is dialled. We understand from the dominant fixed line telephone company that, at present, CLI is only used to keep records of overseas calls for billing purpose. It would be extremely expensive to keep CLI data on all calls as the amount of records to be kept everyday would be enormous. In addition, we are not sure if this option is technically workable. A dial-up account caller would need to call an ISP's number to access the Internet and would be assigned an IP address by the ISP's system. It is questionable if it is feasible to attempt the pairing of the IP address and the caller identity after the event.

8.21 Apart from cost considerations, the CLI function is also not fool-proof. The function may be circumvented by the use of pre-paid telephone SIM cards or calling from a PABX system or a cyber café etc. In addition, if an overseas ISP is involved in the Internet transaction, the CLI function would not be of much help unless that overseas ISP also keeps caller identity records at its end. As pointed out in para. 8.18, however, the Working Group is not aware of any jurisdiction requiring their ISPs to keep caller identity records on an across the board basis for all Internet transactions.

8.22 On balance, therefore, we ***recommend*** that the existing practice of tracing the transactions of specific accounts suspected of involvement in computer crime on a need basis only should continue. In addition, ISPs should be encouraged to keep log records including the calling numbers as a good management practice. However, at this stage, the proposal to impose a mandatory requirement for all Internet transactions to be tracked by the caller number display function or CLI function should be put on hold. In the meantime, we should examine whether there are

appropriate solutions to the difficulties and possible circumvention methods identified above. We should also build up our caseload of investigations impaired by the lack of caller number display or CLI function.

(c) Digital key

8.23 It has been suggested that all ISP account subscribers should register with and obtain a key from a certification authority of the Public Key Infrastructure (PKI)[10]. The arrangement would prevent people from impersonating others to gain unlawful access to ISP systems. It would therefore enable the establishment of reliable trails in computer crime investigations. However, this would mean that overseas visitors would not be able to access ISP service when they are in Hong Kong as they do not possess the requisite key. Furthermore, the arrangement would be incompatible with the international roaming service offered by ISPs worldwide. We therefore ***recommend*** that while both the Government and ISPs should encourage Internet users to make use of the PKI for enhanced security, the requirement should not be made mandatory.

(d) Log records

8.24 At present ISPs are required to pay PNETS charges[11] to the fixed line telephone companies. Typically, ISPs pass the network usage cost to their customers and the PNETS charges appear as a separate item in the customers' bills. As long as there continue to be such charges, ISPs will need to keep the log records for dial-up accounts for billing purposes. It is not clear whether the Telecommunications Authority will change the "PNETS charge" mechanism in the near future. Even if the mechanism

---

(10) The Public Key Infrastructure is an information security arrangement that enables parties to electronic transactions to, through the use of digital certificates and the services of certification authorities, authenticate the identity of other parties to the transactions, ensure the integrity and confidentiality of the information during the transmission process, and guard against the repudiation of the transactions involved.

(11) The Public Non-exclusive Telecommunications Service (PNETS) charge is an interconnection charge paid by the value-added services (VAS) providers, including ISPs, to the local fixed line telephone companies to cover the cost for the use of the fixed networks in connecting the customers of the VAS to the service provider's facilities in a "dialled-up" access. The level of the PNETS charge for the dominant fixed line telephone company is set by the Telecommunications Authority.

is changed, presumably ISPs will still have to keep some kind of log records for audit purposes. This is because their main source of revenue will then be from advertising sponsors, who will need to know the usage rate of the ISPs' service. It may therefore be the case that log records showing at least the time of logging in and out as well as the IP address assigned will still be kept for some time to come. We ***recommend*** that ISPs be encouraged to keep these records for a reasonable period of time, for example, six months.

(e) Summing up

8.25 If overseas experience is any guide, mandating the keeping of records by ISPs appears to be rather uncharted waters. Specifying the types of records that should be kept and the duration for which they should be kept are even rarer. According to legal advice, ISPs may only be compelled to maintain records required by law enforcement agencies by introducing new legislative powers. But this could have various data privacy and other legal implications.

8.26 Taking into consideration the present practice of ISPs, the cooperative attitude of the industry, the social and financial costs of compliance, the lack of overseas experience in this regard and legal concerns, we do not consider it appropriate at this stage to compel ISPs to maintain records. Instead we ***recommend*** that administrative guidelines on record-keeping should be drawn up for ISPs to follow. These should be geared towards guiding ISPs to provide the right kind of assistance to law enforcement agencies. In addition to such matters as subscriber details, caller numbers and log records (paras. 8.14 to 8.24 above), they could lay down steps to standardize the current practices of the law enforcement agencies in their requests for information. That way ISPs may be able to respond to our requests faster. We further ***recommend*** that these guidelines be drawn up in consultation with representatives of ISPs.

8.27 Once the guidelines are in place, we ***recommend*** that they be given suitable publicity. In particular, ISPs should be encouraged to provide a statement or checklist of the extent to which they comply with the

guidelines. Consumers should be encouraged to choose ISPs who adopt the good management practices set out in these guidelines.

(II) Other issues

(a) Take-down procedures

8.28 We believe that, like other content providers, ISPs should be responsible for any contents that they may provide. However, as carriers, ISPs should in principle not be responsible for the contents of messages or sites that they merely carry.

8.29 At present, ISPs would likely remove an offending site known to be under investigation by the law enforcement agencies. Strictly speaking, and depending on the terms and conditions of service of individual ISPs, they may be civilly liable for taking down the site before an offence has been proved. Given that legal proceedings may take some time to complete, however, it might be useful for an offending site to be taken down more quickly so that it will not continue to offend. The Working Group has therefore considered if an approach similar to the US Digital Millenium Copyright Act (para. 8.12 above) should be adopted to better clarify ISPs' legal liability in such situations.

8.30 We consider that, prima facie, a take-down procedure would give a firmer legal ground for ISPs to remove suspected offending materials and sites and should be endorsed in principle. There are two options in realizing this. First, since the main concerns here are copyright infringing articles, illegal gambling operations and pornographic materials transmitted through the Internet, it might suffice for these to be dealt with in the policy context of copyright protection, Internet gambling and control of pornographic materials respectively. Indeed, we note that a similar approach has been adopted in the consultation paper *"Protection of Youth from Obscene and Indecent Materials: 2000 Review of the Control of Obscene and Indecent Articles Ordinance"*. Second, a general enabling provision to empower ISPs to remove offending materials on notice that they are under criminal investigation might be considered. The latter

option would be more comprehensive. However, it might be seen as casting the net too wide. By not limiting the power to specific offences, the provision might be subject to abuse and censorship concerns might arise. On balance, the Working Group is in favour of the first option, and ***recommends*** that the relevant Policy Bureaux should examine the feasibility of putting in place take-down procedures for the respective subjects of copyright protection, Internet gambling and pornographic materials.

(b) Multiple log-in

8.31 At present, many ISP systems set the default in such a way as to allow multiple log-in by their users, i.e., a dialled-up account may be accessed by multiple users at any one time. There are advantages for the account holder, as he has to pay the subscription fee for only one account, while both he and his associates may access the Internet either at different times or at the same time. However, where an account is being accessed without authority, the account holder will not know readily, as he may continue to access the same account at the same time. Whilst the multiple log-in facility offers some convenience to some users, many users do not need such a facility and it is likely that some are not even aware of it. Since the facility carries some security risk, we ***recommend*** that ISPs be encouraged to set their system default to deny multiple log-in, and instead offer the facility only as an option.

(c) Credit limits

8.32 The Working Group believes that individual credit limits are essentially a matter between the cardholder and the issuing bank. Recent developments indicate that the credit card industry is indeed beginning to develop new products for on-line shopping. For example, some leading banks already offer credit accounts with much lower credit limit than normal for use on the Internet. This should reduce the magnitude of loss to the cardholder in case his credit card details are abused in Internet fraud. The use of smart cards, thus obviating the need to key in any credit card detail for on-line transactions, is also starting to catch on.

This market-led approach for dealing with credit limits for on-line shopping should continue. Again we consider that this is not a matter which requires legislation.

(III) Feedback from and cooperation with ISPs

8.33 A safe environment in which to conduct Internet transactions is what legitimate Internet users should be entitled to expect. It should therefore be the common goal for both ISPs and law enforcement agencies alike. In addition, in some cases ISPs are themselves the victims of computer crime. There should therefore be much incentive for ISPs to contribute to combating and preventing computer crime. Their input will particularly be useful when it comes to assessing proposals against the operating environment of ISPs not only in Hong Kong but also globally. To enhance communication between law enforcement agencies and ISPs, and to encourage exchange of ideas on cyber security, we would ***recommend*** –

(a) that a forum of exchange be set up for ISPs and law enforcement agencies to discuss matters of mutual concern at regular intervals. This mechanism should deal with macro issues. For example, one of its first tasks could be the drawing up of the administrative guidelines proposed in para. 8.26; and

(b) that a contact point system be established for dealing with computer crime investigation requests. Each ISP and law enforcement agency should designate contact persons for the purpose. These contacts should each be familiar with the procedures involved in handling a computer crime investigation involving an ISP. The system would enable the contacts to better prioritize individual requests, and would facilitate communication between the two sides. This system may be a sub-set of the exchange forum proposed in (a) above.

Chapter IX

Protection of Critical Infrastructures

Introduction

9.1 This chapter examines the computer related security and law enforcement issues of our critical infrastructures, and evaluates the need for enhanced protection measures to take into account the developments of the information age.

Present position

9.2 There are in every society critical infrastructures whose services are vital to sustaining the smooth operation of the economy and government. If these systems are disrupted or compromised in any major way, there will be a serious negative impact on the workings or even the stability of large parts of the community. Examples of critical infrastructures include power supply systems, fresh water supply systems, public transportation networks, communications networks, essential public hygiene systems and national defence systems.

9.3 At present, there is no defined list of critical infrastructures in Hong Kong. Nonetheless, the utilities, public transport operators such as the Mass Transit Railway and communications network operators take various security measures to protect their premises or facilities against physical attacks. The Police collect, process and disseminate intelligence in this regard and work in collaboration with the infrastructure operators to deal with security incidents.

9.4 In respect of contingencies or disasters, Hong Kong has a three tier Emergency Response System (ERS) to deal with all emergency situations which threaten life, property and public security. In addition to natural disasters, ERS covers incidents arising from the malfunctioning of major systems impacting on our daily life. The response triggered depends on the scale of the contingency in question. For a smaller-scale contingency, the Tier 1 Response, with emergency services still operating

entirely under the coordination of their own commands, may be sufficient. This is the business as usual situation as actions by Government departments are in accordance with their own laid down routine procedures. In the event of a major incident involving widespread threats to life, property and security where extensive coordinated Government emergency response operations are required, the Tier 3 Response will be activated. The Emergency Monitoring and Support Centre will be activated as a central mechanism to facilitate coordination of emergency responses by individual commands. Where necessary, the level of oversight and the manning scale may be escalated.

9.5 Hitherto the security concern relating to critical infrastructures has mainly been physical. Traditionally, the focus of our approach to the protection of critical infrastructures has been on preventing or coping with physical attacks on a more or less stand-alone basis (perimeter defence). The rapid development in computer technology and the society's increasing reliance on the Internet for communication, commerce, research and leisure purposes have however added a new perspective to the assessment of the security of our critical infrastructures. How secure are they in the cyber world? Has the interconnectivity that facilitates interaction through the Internet and telephone lines provided new opportunities for criminals or terrorists to invade classified records, engage in information warfare or disrupt a critical infrastructure's operation? In short, is there a need for more attention to be paid to the interdependence of our infrastructures in the borderless regime of the cyber world?

9.6 There have been in other jurisdictions examples of criminals and terrorists using information technology to invade or disrupt critical infrastructures. For instance, between 1986 and 1989, a group of West German hackers stole passwords and information from various military and industrial computers in the US and Japan and sold them to the Soviet KGB (Secret Service). There are numerous examples of the servers or homepages of foreign government departments and agencies or public utilities being hacked into or otherwise compromised (e.g., by denial of service attacks). Theoretically, someone with a computer, a modem, and a telephone line anywhere in the world could, say, shut down an

airport's air traffic control system, disrupt the emergency services of an entire community, or even activate missile systems if these are linked, directly or indirectly, to the Internet or a telephone line.

9.7 To some extent, there has already been some recognition of the new concerns. In Hong Kong, the Information Technology Services Department (ITSD) takes the lead to ensure the security of the Government computer network. However, critical infrastructures are mostly not Government-run. As regards the ERS, it is a largely reactive mechanism geared towards dealing with major disasters on a one-off basis. We need to find out if the existing protection measures in Hong Kong are adequate to deal with the new concerns. In the information age, protection of our critical infrastructures requires enhanced speed, more coordination and more frequent review and updating of both protection and contingency plans. The traditional incident- and installation/facility-specific, and reactive approach needs to be supplemented.

Examples in other jurisdictions

(a) Critical infrastructure protection

9.8 Available literature on the subject mainly centres on the US experience. The main features of the US policy on critical infrastructure protection announced in 1998 are as follows –

- formulation of a coordinated National Infrastructure Assurance Plan covering both the public and private sectors at all levels;
- establishment of a national center which serves as a critical infrastructure threat assessment, warning, law enforcement and response unit;
- creation of a national unit which assists national education and awareness programs, and coordinates legislative and public affairs; and

- encouraging the private sector to set up liaison centers to pass on security information to and from the national center and their industries.

The implementation details of the policy are set out at **Annex 7**.

9.9 In January 2000, the first US National Plan for Information Systems Protection was published. The plan includes 10 programs which aim to achieve three broad objectives – "prepare and prevent", "detect and respond" and "build strong foundations". The programs are –

- Identify critical infrastructure assets and shared interdependencies and address vulnerabilities.
- Detect attacks and unauthorized intrusions.
- Develop robust intelligence and law enforcement capabilities to protect critical information systems.
- Share attack warnings and information in a timely manner.
- Create capabilities for response, reconstitution, and recovery.
- Enhance research and development in support of the programs.
- Train and employ adequate number of information security specialists.
- Outreach to increase awareness of the need for improved cyber security.
- Adopt legislation and appropriations in support of the programs.
- In every step and component of the Plan, ensure the full protection of civil liberties, rights to privacy and rights to the protection of proprietary data.

(b) Emergency response

9.10 According to the US model, emergency response is part and parcel of an overall critical infrastructure protection plan. There are also examples in other economies, however, of computer emergency response teams (CERTs) operating as free-standing outfits with no immediate linkage to a bigger critical infrastructure protection plan. The specific functions of CERTs may vary from one jurisdiction to another. However, the core functions typically include the collection, sanitization and dissemination of information and warnings in relation to threats to computer networks taking the forms of hacking and computer viruses. Ancillary functions include public education to raise awareness of computer security issues and preventing security breaches. In addition, some CERTs offer value added services by providing remedies for problems of individual computer systems. **Annex 8** sets out further details of the functions of some overseas CERTs.

Consideration

(a) Need for information security/assurance

9.11 For any organization that uses information technology in its day to day operation, ensuring the security of both the information system(s) as well as the information itself should be part and parcel of its organizational strategy. A high level of information security or assurance contributes to the effective and successful achievement of the organization's objectives. Conversely, lax information security could result in massive losses for the organization in terms of, for example, goodwill, profit and productivity, and could threaten the very survival of not only the organization itself but also the well-being of others who have to deal with it. For instance, if a company is subject to repeated denial of service attacks, its ability to retain the confidence of its customers, suppliers and creditors alike will drop. If the patient data in a public health system is mixed and scrambled, large-scale re-screening and re-testing will be required before operations may be performed or prescriptions made. The unauthorized disclosure of confidential information ranging from criminal investigation intelligence to commercial negotiations could

seriously jeopardize the interests of not only the victim of the unauthorized access but also other parties involved.

9.12 Information security or assurance therefore includes three basic elements –

- reliability of access for authorized parties – service and data are available when required, with the identity of the users duly verified and authenticated;
- integrity of data – data is free from contamination; and
- confidentiality – information is restricted to authorized parties only.

Thus analyzed, it is clear that the main determinant of information security resides in and among user organizations themselves. It is important that they have a policy that seeks to ensure information security. This policy should be drawn up having regard to the needs of the organization involved, and it should be backed up by the necessary resources (human capital as well as technical equipment and software) and procedures. Apart from ensuring its own information security, the Government mainly plays the role of a facilitator and promoter in this area. It provides the necessary regulation for dealing with unlawful breaches. It fosters the growth of the information infrastructure, including such features as the public key infrastructure. In addition, it promotes awareness of the issues involved through its education efforts (please see Chapter X). However, it does not, and cannot, supplant the role of the management of the myriad organizations in the community in ensuring information security for their own organizations.

(b) Critical infrastructure protection

9.13 Much of the consideration in paras. 9.11 and 9.12 above applies to our critical infrastructures. The responsibility for ensuring their information security rests with their operators. Nonetheless, in view of the special significance of critical infrastructures to society in general, the Government has a legitimate interest in ensuring that their information

security plans keep up with the requirements of evolving circumstances. The Working Group has therefore looked into the question of critical infrastructure protection in some detail.

9.14 In principle, our critical infrastructures should be equally equipped for tackling physical as well as virtual or cyber attacks. Indeed, with the development of technology, there is increased inter-dependence (not necessarily inter-connection) of the different systems. A general power failure for a prolonged period, for example, could seriously affect our water supply and transportation systems, and much more so than, say, a few decades ago.

9.15 At this stage, we should not preclude the possibility that the protection and contingency plans already in place for our critical infrastructures are basically adequate to tackle possible cyber attacks or computer sabotage, or will be so with some minor adaptation. However, to the Working Group's knowledge, no overall assessment in this regard has been made. In addition, even if protection and contingency plans are in place for individual facilities, there is no coordination of these plans. Weak links or mismatches may well be present.

9.16 It is therefore essential to find out, at an early stage, what the present situation is and to identify the vulnerability areas. Based on the United States' experience, the task is clearly beyond the Working Group's capability to undertake(12). As a first step, therefore, we ***recommend*** that a thorough assessment for the purpose be undertaken. This assessment would need to –

- identify the infrastructures to be studied;
- determine if protection, contingency and recovery plans are in place to guard against cyber attacks in respect of the installations/facilities/systems in question, both individually (for stand-alone systems) and collectively (for inter-dependent or

(12) The US President's Commission on Critical Infrastructure Protection was made up of some 20 members and over 60 supporting staff. It took 16 months to complete its report.

networked systems);

- conduct threat/vulnerability assessments; and
- evaluate the adequacy of the above plans against the threat/vulnerability assessment results.

9.17 While we would not wish to prejudge the outcome of the initial assessment, we believe that it will likely find that our current preparedness is inadequate. Even if individual plans are adequate in themselves, there is no coordination at the macro level. With highly inter-independent critical infrastructures, this is arguably a weak link in itself. Where the infrastructures are run commercially, considerations of the balance sheet bottom line and of keeping an edge over one's competitor also mean that protection against potential cyber attacks may not always receive the priority that it deserves. We therefore ***recommend*** the establishment of a standing central mechanism capable of coordinating the preparation and synchronization of protection, contingency and recovery plans against computer and Internet-related security threats to our critical infrastructures. The appropriate organizational structure of such a mechanism will need to be further considered in light of the mismatches or inadequacies to be identified in the existing mechanism. As a general principle, however, the mechanism's work should dovetail with the existing mechanism for protection, contingency and recovery in response to major emergencies and draw on available expertise as far as possible. It may well be the case that the cyber and physical parts have to work in tandem and should be merged into one effort. For example, the Government periodically mounts inter-departmental exercises to test the effectiveness and efficiency of the ERS in dealing with emergency situations. These ERS exercises should include scenarios of cyber attacks to our critical infrastructures with a view to testing and strengthening our preparedness.

9.18 The Working Group ***recommends*** the following core functions or objectives for the standing central coordinating mechanism to protect our critical infrastructures from cyber attacks –

- identify and regularly review the list of critical infrastructures;
- ensure that individual critical infrastructure operators will carry out threat and vulnerability assessment of their infrastructures vis-à-vis cyber attacks;
- coordinate threat and vulnerability assessment of inter-dependent critical infrastructures vis-à-vis cyber attacks;
- ensure individual critical infrastructure operators will prepare and regularly update protection, contingency and recovery plans for their own critical infrastructures in response to possible cyber attacks targetted at individual infrastructures;
- coordinate the preparation and regular updating of protection, contingency and recovery plans for inter-dependent critical infrastructures in response to possible cyber attacks; and
- coordinate or take part in coordination of emergency response in the event of a cyber-attack induced incident.

The emphasis should be on better coordination across the board, and not on creating another bureaucratic layer. A possible example is the coordination of efforts in response to the Y2K problem.

9.19 Needless to say, this central mechanism will need to work closely with critical infrastructure operators in both the public and private sectors. In addition, to carry out its core functions properly, it should maintain close and frequent contact with both relevant local and overseas bodies on information security. Other ancillary functions could include working with industry associations to promote information security awareness among private sector firms.

(c) Emergency response

9.20 We understand that there have been two applications for funding seeking to set up a CERT in Hong Kong, namely from the Hong Kong Productivity Council and the Information and Software Industry

Association. The Information Technology and Broadcasting Bureau (ITBB) would facilitate the establishment of a CERT in Hong Kong.

9.21 The ability to swiftly raise awareness of a computer virus or hacker attack would contribute to containing the spread of the problem. A CERT is also likely to be able to provide useful information on computer crime trends and developments, and possibly even leads for tracing victims and perpetrators. A CERT should be useful whether or not there is a separate and more focussed mechanism targeted at protecting our critical infrastructures from cyber or computer-induced attacks. In principle, therefore, the Working Group ***supports*** the setting up of a CERT in Hong Kong from the point of view of law enforcement facilitation.

9.22 We ***recommend*** that our critical infrastructure operators be covered by the CERT if and when the latter is set up. We also ***recommend*** that, pending the establishment of the CERT, liaison has to be increased between the Information Technology Services Department and critical infrastructure operators to enable the prompt sharing of information to better deal with emergency situations. Communication steps should be cut down as far as possible.

Chapter X

Public Education

Introduction

10.1 This chapter reviews existing efforts by the Government and other public sector organizations to educate the public of the importance of and measures for preventing and detecting computer crime. It also examines whether and how our current education efforts should be improved.

Present situation

10.2 Prevention is part and parcel of any comprehensive effort to combat crime. This is particularly true with computer crime, where public education plays a key role through raising security awareness and promoting ethics. For example, computer users in general would benefit from increased knowledge of measures to protect their computer systems from hacking attempts. Administrators of networked computer systems would need to ensure that they observe good management practices in maintaining their systems. Parents and teachers would require special tools to protect their children and students from the influence of pornographic materials. E-shoppers would need advice on how to avoid fraudulent on-line traps. These are just a few of the many examples of the importance of increased security awareness.

10.3 The importance of ethics is underlined by the fact that, in the information age, an increasing number of daily transactions in virtually all sectors are dependent on the Internet or are handled by computers. The highly inter-connected nature of networked computer systems means that one single attack could wreak havoc with thousands of systems globally, leading to enormous losses in both monetary and productivity terms. The "Love Bug" attack in May 2000 is estimated to have caused losses amounting to US$10 billion, for example. The sad fact is that in many

cases the attacks are mounted by people who may have no particular grudge against the attack targets and who may gain nothing more than "fame" in the hacker community from the attacks. It is therefore critically important to drive home the seriousness of such computer crime through education, especially of our younger generation.

Current efforts

10.4 At present, a number of agencies are already involved in publicity and education efforts on information security and computer ethics. The message is usually disseminated through –

(a) school talks;

(b) briefings for firms;

(c) public seminars;

(d) exhibitions;

(e) curriculum reviews;

(f) web sites; and

(g) industry guidelines.

A fuller description of the various efforts of individual agencies is at **Annex 9**. It can be seen that whilst most of the efforts are mounted on a stand-alone basis, there are also instances involving multi-agency participation.

Consideration

10.5 The Working Group is encouraged by the numerous efforts of the various agencies in promoting the importance of information security awareness and ethics. It is evident that much has already been done, and much will continue to be done. Put together, the efforts already cover, broadly, the relevant themes and audiences. It is also reassuring to note the various

attempts at cooperation among different agencies in organizing some of the education and publicity initiatives.

10.6 Nonetheless, the Working Group considers that there is room for improvement with the present arrangement. Currently the individual efforts are strong in spontaneity, but relatively weak in terms of coordination. For instance, two or three different agencies may be conducting separate talks to the same school and making different but overlapping proposals as regards curriculum amendments, or multiple agencies may be setting up different booths at the same exhibition to promote information security awareness. Improvement should therefore be geared towards both optimizing the use of limited resources and maximizing the effect felt at the receiving end. Consideration should be given to pooling the agencies' resources and input for better results. Increased dialogue on an inter-agency level would also enable the agencies involved to better share information amongst themselves and encourage them to take an overall view.

10.7 The Working Group therefore ***recommends*** the establishment of a mechanism involving all Government departments and other public sector organizations such as the Productivity Council and the Consumer Council which are engaged in education or publicity efforts on information security. Once the CERT is set up (please see Chapter IX), it should also be involved in the process. We envisage the following broad framework for the proposed mechanism –

(a) The mechanism should provide a common forum for participating agencies to share information on their education or publicity programs in the pipeline.

(b) Participating agencies will continue to have primary responsibility for drawing up and implementing their own education or publicity programs. Through the information-sharing mechanism, they should allow and encourage participation in and contribution to

these programs by other agencies where possible. For the purpose, the lead agency should give sufficient advance notice of the programs that it is planning for.

(c) The mechanism should enable participating agencies to assess how their efforts and programs fit in with the bigger picture. It should therefore be well placed to serve as the focal point for mapping out the public sector's overall education and publicity strategy on information security. Individual programs should dovetail with and support the priority areas and themes of this strategy. Wherever possible, the pooling of resources should be encouraged in place of compartmentalization of efforts.

(d) The mechanism should coordinate the mobilization and involvement of the private sector in public sector-led education and publicity programs on information security, and vice versa. (Please see Chapter XI on the private sector's role in education and publicity efforts.)

Chapter XI

The Private Sector's Role

Introduction

11.1 Law enforcement agencies cannot fight crime effectively without the participation and assistance of members of the public. This chapter examines the role of the private sector in combating and preventing computer crime.

Present position

11.2 As set out in paras. 9.11 to 9.12, Chapter IX, each organization has its own responsibility in ensuring information security. Indeed, although the public sector is sometimes the attack target, in most cases the victims of computer crime are private sector firms or individuals. The brunt of economic and financial losses caused by such crime is also borne by the private sector. It is therefore clearly in the interest of the private sector to ensure that computer crime is reined in.

11.3 The private sector has indeed responded to the challenge of cyber crime in a number of ways. For example, there are anti-virus software programs either for sale commercially or provided for free, as well as professionals who may devise tailor-made security measures to protect networked computer systems. The copyright industry strives to protect its members' works from being illegally transmitted via the Internet. Filter or "nanny" software programs are available to protect children from the influence of indecent or obscene materials carried on the Internet. Security is also a standard feature in devising Internet browsing programs.

11.4 Nonetheless, it is commonly accepted that, by and large, information security awareness and consequently information security measures still leave much room for improvement. For example, devastating losses and painful reconstruction could have been avoided by making regular backup copies of data. Simple security steps such as changing one's password frequently and not sharing it with others, and logging off from an Intranet environment before accessing the Internet are not always observed. Investment in information security devices has yet to be universally accepted as part and parcel of the essential operating cost of a commercial concern. Similarly, respect for intellectual property rights, and hence the need to use genuine application software programs, sometimes takes second place to cost considerations.

Consideration

11.5 As regards ***information security devices or programs***, the examples in para.11.3 indicate that the private sector is indeed capable of coming up with various responses without much, if any, government assistance. Since the private sector is close to the market, it may respond quickly to the needs of consumers, be they big corporations or private individuals. We see no reason to change this essentially market-led approach.

11.6 Nonetheless, we consider that the Government may still play a role in this area, and this relates to information sharing. In the course of investigating a computer crime, law enforcement agencies may obtain detailed information on how security has been breached. We ***recommend*** that such information should be fed back to the relevant industries, such as the software industry and telecommunication device manufacturers, for follow up. Concomitantly, the private sector should keep the law enforcement agencies abreast of trends and developments in information security, and share their security concerns. Depending on the case nature, this may be done either individually (involving only particular firms) or collectively (involving industry associations or representatives). We would like to stress, however, that the sharing of

information within the private sector itself is equally if not more important. Chambers of commerce, professional organizations and industry associations should all organize initiatives in this regard.

11.7 The Working Group considers that the private sector should be able to play a bigger and more active role than now in respect of ***education and publicity*** on information security. The message itself is simple enough – every user has a responsibility to protect his own computer system and data. For the message to filter through and given effect, though, we cannot rely on the Government alone. The private sector has a natural role to play in education and publicity efforts at various levels, for example –

(a) within particular industry sectors – professional organizations and industry associations may draw up codes of practice or organize security seminars tailored to their own industries;

(b) across sectors – chambers of commerce, representatives of small and medium enterprises or relevant statutory organizations may develop guidelines or help lines for small and medium businesses;

(c) between industry and consumers – service providers (e.g., banks, Internet service providers and e-retailers) may proactively disseminate security information to their clients; and

(d) more generally, across the community – various stakeholders may organize activities to increase information security awareness.

The central theme is the need to ensure information security (reliability of access, integrity of data and confidentiality of data) (please see Chapter IX). The detailed efforts will of necessity vary with the different levels involved, and should typically evolve around –

(a) the importance of information security as an integral part of corporate strategy;

(b) computer use ethics;

(c) precautionary security measures to minimize the chance of attacks and limit the damage in case of attacks;

(d) best management practices or codes of practice for particular industries, e.g., e-banking, e-retailing;

(e) the importance of security features in product development (particularly relevant to the information technology and copyright industries, for example);

(f) the importance of information sharing; and

(g) the need to cooperate with law enforcement agencies – reporting computer crime, providing feedback etc.

11.8 We ***recommend*** that the private sector should be encouraged to undertake more education and publicity efforts at various levels around the key theme along the lines set out in para. 11.7. In particular, professional organizations, industry associations and chambers of commerce should be encouraged to contribute to the total effort.

11.9 While there is much that the private sector may and can do on its own in terms of education and publicity, there continues to be scope for the Government and other public sector organizations to take part in private sector-led initiatives and vice versa. We ***recommend*** that, where resources permit, the relevant Government and public sector agencies should lend as much support to private sector-led initiatives as possible. Similarly, for education and publicity programs organized by Government or public sector agencies, we ***recommend*** that the concerned agencies should actively involve the private sector. Such involvement may take the form of contribution in cash as well as in kind (including ideas). (Please see Chapter X.)

11.10 Given that the private sector is not only closely affected by, but also plays an important part in determing the effectiveness or otherwise of, Government policies on computer crime, it should have a legitimate interest in the formulation of these policies. The Working Group ***recommends*** that the Government should continue to involve the private sector in such ***policy formulation.*** We note that to a large extent, this is already the current practice. In addition to the general public, the relevant industries are consulted on proposals impacting on them directly, e.g., Internet service providers are consulted on the problem of the transmission of indecent and pornographic materials over the Internet. We have nonetheless considered if more steady input from the private sector should be sought on a more regular basis. Should there be a tripartite forum involving representatives from the Government, relevant statutory organizations and the private sector to discuss computer crime issues, for example? The upside is that this would enable a more macro look at the overall picture. The downside is that such a forum on its own could be seen as a talkshop and might not achieve much in practice.

11.11 On balance, we believe that it would be more useful to seek private sector input in the context of discussing and considering substantive issues instead of generalities. It would be more productive to factor in private sector input in the overall institutional arrangements to deal with computer crime issues than having a dedicated forum for the sole purpose of soliciting private sector input. The question of overall institutional arrangements will be addressed in Chapter XIII. Subject to agreement to the thrust of the recommendations therein, we see no need for a stand-alone arrangement for seeking private sector input.

11.12 As awareness of the need for information security builds up, it will be increasingly necessary for security preparedness to be assessed according to some commonly accepted standards. In the longer run, therefore, we ***recommend*** that the feasibility of a commonly accepted ***audit or assessment*** mechanism in respect of information security standards for different industries and at different levels be explored. This could take

the form of, for example, a quality mark system with the accreditation body being an industry association, professional body or a stand-alone entity. Only firms complying with specified security standards for their information systems will be accorded the quality mark or certification. The CPA WebTrust[13] program being promoted by the Hong Kong Society of Accountants is an example in this direction. The accreditation or certification idea will of necessity have to be pursued having regard to international developments in the area. If put to practice, it would be a useful incentive for private sector firms to embrace adequate security measures to protect their information systems both vis-à-vis their business partners and individual consumers. For instance, the adequacy of information security measures could be a factor in considering the insurance premium for a private firm. Similarly, it would feature in the consideration of increasingly discerning consumers when they shop around for providers of goods and services.

(13) The CPA WebTrust is an e-commerce based seal of assurance designed to build trust and confidence among consumers purchasing goods and services over the Internet. The program was developed jointly by the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Public Accountants (CICA) and a provider of digital certificates and encryption services. Websites which have complied with the WebTrust principles and criteria covering both technical aspect such as security and business operational aspects such as minimizing the risk of fraud and protecting customers' personal information, delivering sale promises, may be awarded the WebTrust seal.

Chapter XII

Resources and Capabilities

Introduction

12.1 This chapter reviews the resources at the disposal of our law enforcement agencies for combating computer related crimes and assesses the need for improvement.

Present situation

(a) Departmental efforts

12.2 A Computer Crime Section (CCS) has been set up within the Commercial Crime Bureau (CCB) of the ***Hong Kong Police Force*** since 1993 for the investigation of computer related crimes. The 18-member CCS is also responsible for the centralized forensic examination of computer evidence involved in crimes that are investigated by other Police formations. CCS maintains close contacts with local and law enforcement agencies in other jurisdictions to monitor crime trends and develop investigation skills. A plan is in hand to upgrade the level of command and substantially expand the strength of the CCS by mid 2001.

12.3 For the purpose of broadening the computer crime investigative capability of the Police, a Computer Crime Investigation Cadre (CCIC) comprising 83 officers from various districts and other formations has been formed since December 1999. They assist in computer crime investigation in frontline formations, including the seizure of computer exhibits and initial assessment of the computer crime scene. CCS coordinates the deployment of CCIC, provides the necessary technical support to the latter's investigations and deals with the more serious or transborder cases.

12.4 CCS organizes a Computer Crime Investigation Cadre Course for members of the CCIC and officers from other interested law enforcement agencies. The one-day course is held on a monthly basis to provide trainees with up-to-date knowledge on investigations into computer crimes.

12.5 CCS is in the course of setting up a Computer Forensic Laboratory to facilitate the forensic examination into digital evidence recovered from computer exhibits seized in criminal investigations. An initial sum of $ 2.7 M has been allocated to the project for the procurement of the necessary hardware and software.

12.6 The Crime Prevention Bureau has set up a Computer Security Unit for providing computer crime prevention advice to companies, schools and individuals.

12.7 In the area of international cooperation, CCS maintains contacts with a large number of agencies and organizations, both locally and outside of Hong Kong. They include liaison officers of Japan, the US, Canada and the UK based in Hong Kong and computer crime investigators in Singapore, the US and the UK.

12.8 The ***Independent Commission Against Corruption*** (ICAC) has established a Computer Forensics and Research Development Section (CFRDS) since April 1999. In addition to computer forensic examination work, the 7-officer section is responsible for external liaison on computer forensic matters and arrangement of computer forensic training for ICAC officers.

12.9 The CFRDS organizes one-day in-house training courses for ICAC investigators covering the basic principles of computer forensic examinations and the procedures in searching and seizing computer exhibits.

12.10 ICAC has established informal contacts with computer crime experts of law enforcement agencies in Canada, the US, the UK and Singapore.

12.11 An Anti-Internet Piracy Team, consisting of 7 officers, has been formed within the Intellectual Property Investigation Bureau (IPIB) of the ***Customs and Excise Department*** (C&ED) since January 2000 to investigate complaints about intellectual property rights infringement activities on the Internet.

12.12 C&ED has established contacts with US and UK agencies specializing in computer crime investigation.

12.13 In the ***Immigration Department***, arrangements are in hand to set up a computer crime investigation unit to handle forgery of travel documents by means of the computer.

12.14 The ***Department of Justice*** has established a Computer Crime Section within the Commercial Crime Unit of the Prosecutions Division since January 2000 to handle computer crime cases. Its primary duties include the provision of legal advice to law enforcement agencies regarding criminal charges to be laid in the area of computer crimes and the actual conduct of such prosecutions in the courts. Hitherto, the unit relies on the CCS of the Police to obtain information from overseas agencies and has not established liaison channels with its counterparts in other jurisdictions.

(b) Cross-agency efforts

12.15 The Police, ICAC and Hong Kong University of Science and Technology (HKUST) joined hands to form the Computer Forensic Working Group in late 1998 to devise a professional computer forensic training program.

12.16 A Computer Crime Investigation and Computer Forensic Examination Course was held between 7 and 25 January 2000 and attended by 23 officers from the Police, ICAC, C&ED, Immigration Department and the Department of Justice. The course sought to pool together systematically the latest developments in computer forensics on a cross-agency basis and is the first of its kind in Asia. Three more such courses were held in June and July 2000 and attended by 28 officers from ICAC, C&ED, DoJ and Inland Revenue Department. Consideration is

being given to organizing similar training courses in January 2001.

Consideration

12.17 The Working Group is encouraged by the initiatives taken by the various law enforcement agencies to respond to the challenge of computer crime over the past few years. We note, for example, that most of the dedicated units on computer crime have been set up for a fairly short period of time. ***Staffing and equipping*** these units is of course subject to the usual procedures of resource allocation. We would nonetheless like to ***stress*** the importance of ensuring that sufficient resources are provided for the effort to combat and prevent computer crime, not only for the dedicated units, but also for other units and formations involved in the process. Computer criminals have access to the latest available technologies on the market. If our law enforcement agencies cannot catch up, their capability to detect computer crime will certainly be hampered. Flexibility in procurement should be allowed as far as possible.

12.18 Computer crime investigation and computer forensic examination involve rather specialized ***expertise***. We have therefore considered whether adequate steps are in place to ensure that there are sufficient pools of expertise to meet increasing demands. We are reassured by the law enforcement agencies' representation that sufficient backup is available. Nonetheless, if overseas experience is any guide, the government often has to compete with the private sector for expertise in this field. In addition, we should cater for staff movements for career development. We would therefore ***urge*** that these agencies should continue to keep the situation under close review to ensure that there is no mismatch between the demand for and supply of relevant expertise. We would also ***suggest*** that private sector resources and cooperation be leveraged on as far as possible. For instance, exchange programs may be considered.

12.19 The Working Group has considered a suggestion for pooling all resources of our law enforcement agencies in respect of computer crime to form a central ***one-stop unit***. On the face of it, this suggestion might bring about better economies of scale. On closer examination, however, it has

certain shortcomings. Different agencies have different statutory powers and are subject to different constraints in exercising their powers. It would not be possible, without substantial legislative amendments, to entrust a new unit to deal with all crimes perpetrated via the computer. In addition, as pointed out above, even within the same agency, and even if there is a dedicated unit on computer crime, computer crime investigation is not the monopoly of any one unit. It would therefore be very difficult to determine exactly what resources should be pooled into the proposed one-stop unit, and what should be left in the original agency. Unless there was a clear and easily enforceable demarcation of responsibilities, the subsequent extra steps in the communication process could result in delays in handling a case. We are therefore not in favour of the proposal of a one-stop unit, and ***recommend*** that it should not be pursued.

12.20 Nonetheless, the Working Group agrees that it is important for different law enforcement agencies to ***cooperate and share intelligence and experience*** with each other as far as possible. We note that much cooperation and sharing of information is already being done at the inter-agency level as far as investigations are concerned. We would ***recommend*** that this should continue and be deepened. Specifically, this cooperation should include, for example, the sharing of contact lists, the organization of debriefing sessions involving other agencies after an overseas visit on computer crime, the circulation of reports on attendance at an overseas seminar on computer crime and, perhaps most importantly, the sharing of experience gained and lessons learned in dealing with actual cases. To be effective, this exchange should be carried out on a systematic basis. We have in Chapter X examined whether and how cooperation among the agencies regarding their public education efforts should be improved. In Chapter XIII, we will look into the need for a standing arrangement involving, among others, law enforcement agencies to deal with policy issues concerning computer crime. Increased cooperation and information sharing among our law enforcement agencies would complement these efforts.

12.21 ***Cooperation with law enforcement agencies in other jurisdictions*** is critically important in dealing with computer crime, which respects no geographical borders. Mutual legal assistance agreements (please see Chapter IV) have provided a good basis for the procuring of evidence in transborder crime. However, the sheer speed with which computer attacks may spread and the relative ease with which trails may be covered or erased have added a new dimension to the question of international cooperation. A speedy response on all sides is required. This in turn points to the importance of the ability to pinpoint and contact the relevant action party at short notice. We would therefore ***urge*** our law enforcement agencies to step up this liaison with their counterparts outside Hong Kong, with a view to –

- dealing with individual cases promptly;
- sharing experience and know-how; and
- keeping close tabs on relevant developments, including legislative proposals.

We should also seek to contribute actively to multilateral cooperation in combating computer crime, and offer our input to international efforts in this regard as appropriate.

12.22 The ***examination of computer evidence*** requires special handling. Unlike their physical counterparts, technically computer records are "updated" each time they are accessed. Preserving computer evidence by "freezing" the position with a view to having the evidence accepted by the court therefore presents considerable challenge. This is indeed an evolving subject, and to the Working Group's knowledge there has yet to be international consensus on one standard set of procedures for handling computer evidence. Our ultimate aim should therefore be to ensure that Hong Kong's procedures are in line with the international standards once they are available. To that end, our law enforcement agencies should keep close tabs on relevant international developments.

12.23 Nonetheless, in the shorter term, the Working Group believes that we should aim to work out a standard set of procedures for use among all law enforcement agencies in Hong Kong as soon as possible. With the impending establishment of the Police Computer Forensic Laboratory, we ***recommend*** that the laboratory should be entrusted with the task of taking the lead to develop the common standard, in consultation with other law enforcement agencies, the Department of Justice, the universities and relevant professional organizations both locally and outside of Hong Kong. This would avoid duplication of efforts whilst optimizing the use of available resources. Once the common standard is established, it should be publicized among judges (who preside over court cases involving computer crime), the legal profession (who defend or prosecute such cases), and other interested parties such as ISPs (whose assistance may be required in investigating computer crimes).

12.24 Computer forensic examination involves specialist training and expertise. In addition, like the examination of physical evidence, it requires segregation from investigation to ensure impartiality. In the longer run, therefore, consideration should be given to establishing a computer forensic examination unit or laboratory to provide the service centrally. This would also mean better economies of scale.

Chapter XIII

Future Institutional Arrangements

Introduction

13.1 This chapter examines the need for a standing arrangement to deal with computer crime issues.

Consideration

13.2 The Working Group is an ad hoc task force with a finite life span. We do not profess to be able to deal with all law enforcement and crime prevention issues related to computer crime once and for all. It is therefore necessary to consider how best to follow up on the Working Group's proposals, monitor relevant developments as they evolve and assess their impact on our policies and measures. We have examined several possibilities.

13.3 One possibility is for the tasks to be re-absorbed into the mainstream. This is not an unusual route – once a task force has completed its work, in many cases the accepted recommendations may be implemented within the existing framework or structure of division of responsibilities. The main disadvantage of the approach in this case is the continuously fast evolving nature of computer crime, which means that fairly close monitoring of changing developments will be highly desirable. In addition, without a clearly identifiable focal point, it might be more difficult to involve the private sector on a regular basis.

13.4 The second possibility is for a new standing committee on computer crime to be set up. This has the advantage of giving the mechanism a clear identity and focus. With a stand-alone committee, it may also be easier to pool expertise in the subject and to establish contacts with overseas counterparts. However, it may be argued that since in all likelihood much of the real work will be done by the secretariat, another

committee would have little added value.

13.5 The third possibility is to take a middle-of-the-road approach by tasking an existing committee with the necessary overall monitoring role, and entrusting the detailed follow up work to the Government bureaux and departments concerned and other relevant parties. This would ensure quality control whilst not overloading the committee with too many details.

13.6 In respect of the third possibility, the Working Group has in particular considered the work of two existing consultative bodies on crime and information technology matters. The first is the Fight Crime Committee (FCC). Chaired by the Chief Secretary, the FCC is a high level committee with both Government and non-Government representatives for overseeing crime issues in Hong Kong. As and when necessary, sub-committees may be established under the FCC to deal with specific subject matters. The terms of reference and membership of the FCC are set out at **Annex 10**. The second committee of relevance is the Information Infrastructure Advisory Committee (IIAC). Chaired by the Secretary for Information Technology and Broadcasting, the IIAC advises the Government on the policy, regulatory, technical and other issues relating to information technology and telecommunications. Many of its non-official members are drawn from the information technology and telecommunications industries and academia. Its terms of reference and membership are set out at **Annex 11**.

13.7 The third option set out in paras. 13.5 and 13.6 would avoid a proliferation of committees. More importantly, it would enable computer crime issues to be considered against a more general backdrop of relevance (the overall crime scene for the FCC and the development of the information infrastructure for the IIAC). On the latter score, given that the IIAC is more concerned with fostering the growth of the information technology industry than with combating and preventing crime, probably the FCC is a more appropriate parent body.

13.8 The Working Group believes that the objectives set out in para.13.2 (following up on the Working Group's proposals, monitoring relevant developments as they evolve and assessing their impact on our policies and measures) would be better served by an entity which has a fairly clear identity and focus of its own. At the same time, the mechanism would benefit from operating in the overall context of crime prevention and detection. On balance, therefore, we ***recommend*** that, at least initially, a sub-committee under the FCC should be formed to see through the follow up work required. The need for the sub-committee may be reviewed from time to time in light of the progress of its work and developments in computer crime.

13.9 The Working Group has not discussed the detailed arrangements regarding, for example, the exact composition of the sub-committee and how it should be serviced. The final decision regarding these will have to be worked out having regard to such factors as the availability of resources. Nonetheless, we ***recommend*** that the sub-committee should include, among others, senior representatives of law enforcement agencies who have an overall view of both the policy and operational aspects of computer crime. In addition, there should be some private sector representation because of the impact of computer crime on the private sector. (Please see Chapter XI on the private sector's role.)

Chapter XIV

Conclusion

14.1 In this Report, the Working Group has outlined a possible framework for improving the existing regime of measures to tackle computer crime. This framework is certainly no panacea, and we have pointed to some of the limitations in previous chapters. Nonetheless, it should hopefully provide a basis on which future work may be done.

14.2 Given the transborder nature of computer crime, we have been mindful of the need to ensure that our proposed framework is in line with current international thinking on the subject. We have therefore drawn reference from international examples where available in considering each individual topic. To further ensure completeness, we have also attempted a comparison between the Draft Convention on Cyber-crime of the Council of Europe(14), a major initiative to crystallize international thinking on computer crime, on the one hand and Hong Kong's position on the other hand. A checklist for the purpose is at **Annex 12**. It can be seen that our existing measures, coupled with recommendations of the Working Group, are by and large in keeping with the spirit of the Draft Convention's proposals. We should continue to monitor international developments to ensure that our response to computer crime keeps up with the times.

14.3 In our deliberations, we have found that some of our recommendations may have implications on issues that go beyond computer crime as such. We have in Chapter I as well as the relevant individual chapters pointed to the need to examine these implications. In the longer term, we see a need for the barriers between legislation on computer crime and that on physical crime to be demolished. Our law should ideally be able to cater

(14) The Council of Europe is an international organization with 41 member states. It seeks to, inter alia, strengthen the rule of law throughout its member states by encouraging the adoption of common practices and standards. The Council of Europe published the Draft Convention for public consultation in April 2000. The text of the Convention will be finalized by a group of experts by December 2000 and the Committee of Ministers could adopt the text and open it for signature as early as Autumn 2001.

to the requirements of the information age without regard to whether an act is done via traditional means or in the cyber world.

14.4 Realizing the long term goal in para. 14.3 is certainly no easy task. It may well involve a fundamental review of well-established legal concepts and principles. The question of jurisdictional rules is a good case in point (please see Chapter IV). Such a review will take a long time, and will likely have to be done in tempo with developments in other common law jurisdictions. Pending such fundamental change, we would ***recommend*** that, in general, new legislation or amendments to existing legislation should be drawn with an eye to the requirements of the information age. As far as possible, legislation should be technology- and medium-neutral.

14.5 Given the constantly evolving nature of the cyber world, we cannot afford to stand still in our effort to curb computer crime. We hope that those recommendations of the Working Group accepted by the Government will be implemented as soon as practicable. To maximize public acceptance and cooperation, interested parties should be consulted when the implementation details are being mapped out.

Annex 1

Inter-departmental Working Group on Computer Related Crime

Terms of Reference

Having regard to the rapid developments associated with the computer and Internet, and the potential for them to be exploited for carrying out criminal activities –

(a) identify the challenges to law enforcement, for example, in respect of evidence gathering and prosecution, arising from such developments;

(b) review the adequacy of existing legislation and relevant administrative measures to deal with the challenges identified in (a) above;

(c) examine international developments and trends in this area, and draw lessons for Hong Kong as appropriate; and

(d) make recommendations to address the inadequacies identified, taking into account the need to balance law enforcement facilitation on the one hand and the cost of compliance, financial or otherwise, on the other.

Annex 2

Inter-departmental Working Group on Computer Related Crime

Membership

Security Bureau

Miss CHEUNG Siu-hing (Chairperson)
Deputy Secretary (Special Duties)

Mr. NG Sai-kuen (Secretary)
Assistant Secretary (F1)

Commerce and Industry Bureau (formerly Trade and Industry Bureau)

Mr. Philip CHAN
Principal Assistant Secretary (5)

Mr. Johann WONG
Assistant Secretary (5)A

Information Technology and Broadcasting Bureau

Mr. Alan SIU
Principal Assistant Secretary (C) (until July 2000)

Ms Joyce TAM
Principal Assistant Secretary (C) (from July 2000)

Mr. Paul CHENG
Assistant Secretary (C1)

Home Affairs Bureau

Mr. Vic YAU
Assistant Secretary (5)2

Department of Justice

Mr. Stephen WONG Kai-yi
Deputy Solicitor General (Advisory)

Mr. Richard TURNBULL
Senior Assistant Director of Public Prosecution

Ms Roxana CHENG
Senior Assistant Solicitor General (Human Rights)

Mr. Michael SCOTT
Senior Assistant Solicitor General (General Advisory)

Mr. Eddie SEAN
Ag. Senior Assistant Director of Public Prosecution/
Senior Government Counsel

Ms Anita NG
Government Counsel

Hong Kong Police Force

Mr. Victor Y.K. LO
Chief Superintendent
Commercial Crime Bureau

Mr. Peter G. ELSE
Senior Superintendent
Commercial Crime Bureau

Mr. Albert C.Y. CHEUK
Senior Superintendent
Security Wing

Mr. Y.H. LAU
Superintendent
Security Wing

Mr. Hilton CHAN Kwok-hung
Chief Inspector
Commercial Crime Bureau

Miss IP Ka-yee
Inspector
Commercial Crime Bureau

Independent Commission Against Corruption

Mr. Gilbert CHAN Tak-shing
Assistant Director of Investigation

Mr. Louis CHEUNG Wah-pong
Principal Investigator (K)

Mr. Vitus CHUNG
Chief Investigator (K)5

Customs and Excise Department

Mr. Vincent POON
Assistant Commissioner (Control and Intellectual Property)

Mr. AU YEUNG Ho-lok
Superintendent
Intellectual Property Investigation Bureau

Mr. CHAN Yiu-wah
Assistant Superintendent
Trade Descriptions Investigation Division

Mr. LI Chun-fai
Staff Officer
Legislation Group
Office of Management Services

Mr. Frank SHIU Hok-bun
Assistant Staff Officer
Legislation Group
Office of Management Services

Immigration Department

Mr. LEUNG Ping-kwan
Principal Immigration Officer (Investigation)

Mr. Michael HO Chung-wai
Assistant Principal Immigration Officer

Mr. LO Chiu-chuen
Immigration Officer

Information Technology Services Department

Mr. Stephen MAK
Assistant Director (Infrastructure Services)

Ms Joyce MOK
Chief Systems Manager (Infrastructure Services)

Mr. Stanley CHAN
Senior Systems Manager

Office of the Telecommunications Authority

Mr. Danny K.C. LAU
Assistant Director (Regulatory)

Ms Elaine HUI
Regulatory Affairs Manager

Annex 3

Legislative Provisions with References to the Term "Computer"

Ordinance		Section
Chapter 1	Interpretation and General Clauses Ordinance	S. 88
Chapter 8	Evidence Ordinance	S. 20, 22A, 22B, 54 and 77F
Chapter 41	Insurance Company Ordinance	Schedules 3 and 8
Chapter 52	Television Ordinance	Schedule 1C
Chapter 60	Import and Export Ordinance	S. 20, 21 and 33A
Chapter 61	Loans Ordinance	S. 4
Chapter 106	Telecommunications Ordinance	S. 27A
Chapter 112	Inland Revenue Ordinance	S. 16G, 26A and 51C
Chapter 155	Banking Ordinance	S. 2 and 137B
Chapter 174	Births and Deaths Registration Ordinance	S. 2, 5A, 13, 22, 25, 27 and 32
Chapter 200	Crimes Ordinance	S. 59 and 161
Chapter 210	Theft Ordinance	S. 2, 11 and 19
Chapter 232	Police Force Ordinance	S. 39
Chapter 310	Business Registration Ordinance	S. 19
Chapter 318	Industrial Training (Clothing Industry) Ordinance	S. 31A
Chapter 324	Protection of Non-government Certificate of Origin Ordinance	S. 6A and 10
Chapter 333	Securities Ordinance	S. 2

Ordinance		Section
Chapter 395	Securities (Insider Dealing) Ordinance	S. 2
Chapter 440	Bills of Lading and Analogous Shipping Documents Ordinance	S. 2
Chapter 444	The Hong Kong Institute of Education Ordinance	S. 4
Chapter 445	Layout – Design (Topography) of Integrated Circuits Ordinance	S. 2
Chapter 486	Personal Data (Privacy) Ordinance	S. 8
Chapter 493	Non-local Higher and Professional Education (Regulation) Ordinance	Schedule 2
Chapter 494	Aviation Security Ordinance	S. 58
Chapter 503	Fugitive Offenders Ordinance	Schedule 1
Chapter 514	Patents Ordinance	S. 93
Chapter 522	Registered Designs Ordinance	S. 3 and 8
Chapter 526	Weapons of Mass Destruction (Control of Provision of Services) Ordinance	S. 5, 6, 7 and 9
Chapter 528	Copyright Ordinance	S. 4, 11, 17, 22, 25, 29, 60, 61, 91, 93, 116, 121, 154, 161, 198 and 199 Schedules 2 and 5
Chapter 542	Legislative Council Ordinance	S. 20Z
Chapter 553	Electronic Transactions Ordinance	S. 2
Chapter 1053	University of Hong Kong Ordinance	Schedule

Ordinance		Section
Chapter 1126	Hong Kong Baptist University Ordinance	S. 7
Chapter 1145	The Open University of Hong Kong Ordinance	S. 4
Chapter 1165	Lingnan University Ordinance	S. 6

Annex 4

Production of Computer Information in a Visible and Legible Form : Legislative Provisions

Law	Provisions
S. 88, Interpretation and General Clauses Ordinance (Cap.1)	In relation to material consisting of information contained in a computer, the order issued by the Court of First Instance or District Court to seize journalistic materials requires that the material be produced in a form which is visible, legible and can be taken away. The order also gives an applicant access to the material in a form in which it is visible and legible.
S. 4, Organized and Serious Crime Ordinance (Cap. 455)	For the purpose of the investigation into organized crime, the Secretary for Justice or an authorized officer may make an ex parte application to the Court of First Instance for an order that within a specified period a person who appears to be in control of the material relevant to the investigation to produce the material to an authorized officer or give an authorized officer access to the material. Where the materials in relation to the order consist of information recorded otherwise than in legible form, they have to be produced in a visible and legible form which can be taken away. Any person who fails to comply with the order commits an offence and is liable to a fine of up to $100,000 and to imprisonment for one year.

Law	Provisions
S. 10, Protection of Non-Government Certificates of Origin Ordinance (Cap. 324)	An authorized officer may require any computer information related to an offence under this Ordinance be produced in a form in which it can be taken away and in which it is visible and legible. Any person who fails to comply with the requirement of the authorized officer commits an offence and is liable to a fine of up to $10,000 and to imprisonment for 6 months.
S. 5, Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526) S. 6 & 7, Cap. 526	Any member of the Customs and Excise Service and any authorized officer may require any computer information related to an offence under this Ordinance to be produced in a form in which it can be taken away and in which it is visible and legible. A magistrate may issue a search warrant to a member of the Customs & Excise Service or an authorized officer to search a place for computers which contain information relating to an offence committed under the Ordinance. The officer may require the computer information to be produced in a form in which it can be taken away and in which it is visible and legible.

Annex 5

"Theft" of Computer Data : Cases

Between June and October 1994, a person based in Russia gained access over 40 times to a US bank's cash management system using a personal computer and stolen passwords. Together with his accomplices, they transferred more than US$ 10 million in funds from three customers of the bank to other bank accounts in California and other European countries. This person and four of his accomplices were eventually arrested and tried in the US. They all pled guilty. The US bank was able to recover the majority of the stolen funds.

2. In March 2000, authorities of Wales, the UK, arrested two individuals for intrusions into e-commerce sites in several countries and theft of credit card information of over 26,000 accounts. According to the US FBI, the losses from this case could exceed US$ 3 million.

3. In a case in early 2000 in Hong Kong, three young hackers made use of a computer program to capture the log-in names and passwords of 127 other Internet users who were surfing simultaneously with them. With the help of a distributor, the details of these accounts and passwords were sold to avid Internet gamers for HK$350 each. As a result of the abuses of the accounts, 11 local ISPs reported to the Police that they had suffered a loss totaling HK$197,490. Three culprits were successfully prosecuted and convicted in court.

Annex 6

Types of Records to be Maintained by Internet Service Providers

Indicative Wish List

The following indicative wish list has been drawn up for illustration purposes only. It summarizes the tentative suggestions by our law enforcement agencies as to the types of records that may be usefully kept by Internet service providers.

Subject	Session records	Account records
(a) Dial-Up Access by Modem	• User Name • Log In Time • Log Out Time • Assigned IP Address • Calling Line Number • E-mail Message ID (with corresponding IP Address, Time & Date) • NNTP(15) Posting ID (with corresponding IP Address, Time & Date) • Webpage Address (with last upload time, IP Address and image of the page)	• Subscriber Name (Verified) • HKIC No. or Business Registration/Company Registration No. (Verified) • Subscriber Address • Contact Person • Contact Tel. No. • Account Opening/Closing Date(s) • Type of Service • Type of connection e.g. (i) Leased Line (ii) Dial Up Line (iii) Broad Band WAP • Login ID • E-mail Account Name • Domain Name • Static IP Address (if any) • Payment Instruction: (i) Bank A/C Information (ii) Credit Card Information • Client A/C Configuration e.g. (i) Mail Server Name (ii) Incoming Mail Server Name (iii) Mail Box Capacity

(15) NNTP stands for "Network News Transfer Protocol".

Subject	Session records	Account records
(b) Ethernet/ ATM[16] Broadband Access	Same as Above plus:- • Unique Ethernet/ATM card Identifier	Same as above plus:- • Installation Address • Installation Tel. Line No.
(c) Individual Audit log of clients	• Log In/Out Time • Dynamic IP Address during each login • Intrusion Detection Log • E-mail re-direction	
(d) Mail Messages	• Message contents (read and unread, including attachments) • Message routing history	

(16) ATM stands for "Asynchronous Transmission Protocol" (computer connection over telephone line)

Annex 7

US Experience in the Protection of Critical Infrastructures

National Infrastructure Plan

In each of the major sectors of the US economy that are vulnerable to attack, a senior government officer in the relevant lead agency works together with the private sector to formulate a sector plan by-

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing attempted major attacks;
- developing a plan for alerting, containing and rebuffing an attack in progress and rapidly reconstituting essential capabilities in the aftermath of an attack.

2. In respect of government critical infrastructures, each department appoints a Chief Information Officer who is responsible for information assurance. In addition there is a Chief Infrastructure Assurance Officer who is responsible for the protection of all the other aspects of that department's infrastructure. Each department develops its own plan for protecting its own critical infrastructure. The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism (National Coordinator) is responsible for coordinating the implementation of the overall policy on critical infrastructure protection. He ensures the overall coordination and integration of the various sector plans and government department plans, with a particular focus on interdependencies. Those plans implemented are required to be updated every two years.

National Infrastructure Protection Center

3. The National Infrastructure Protection Center (NIPC) aims at serving as a national critical infrastructure threat assessment, warning, and law enforcement investigation and response unit. It includes elements responsible for training, outreach and application of technical tools. The NIPC consists of investigators from the Federal Bureau of Investigation, United States Secret Services, Department of Defense and other national security investigators experienced in computer crimes and infrastructure protection. It is expected to be the national focal point for gathering information on threats to the infrastructures. It also provides the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts.

Critical Infrastructure Assurance Office

4. The Critical Infrastructure Assurance Office (CIAO) is created in the Department of Commerce to assist the National Coordinator in integrating the various sector plans into the National Plan. CIAO coordinates the analyses of the US Government's own dependencies on critical infrastructures, assists in the development of national education and awareness programs, and coordinates legislative and public affairs.

Information Sharing and Analysis Centers

5. Information Sharing and Analysis Centers (ISACs) are encouraged to be set up by private sector representatives for gathering, analyzing, sanitizing and disseminating private sector information to both industry and the NIPC. The centers also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. An example is the Financial Services Information Sharing and Analysis Center (FS/ISAC) which was set up in 1999. It is a joint public-private industry initiative designed to facilitate the sharing of information about cyber threats to the financial services industry. It enhances the industry's ability to prevent, detect, and respond to attacks on its technological infrastructure by providing an avenue for rapid distribution of information about such threats.

6. The philosophy behind the US approach is that national and economic security has become a shared responsibility between the government and industry. The government must collect appropriate information and share it with industry, whilst the private sector must take reasonable actions to prevent itself from hackers.

Source : The Clinton Administration's Policy on Critical Infrastructure Protection : Presidential Decision Directive 63

Annex 8

Computer Emergency Response Teams

USA

The Computer Emergency Response Team Coordination Center (CERT/CC) at the Carnegie Mellon University works with the Internet community to respond to computer problems, raising awareness of computer security issues and preventing security breaches. CERT/CC was set up in 1988 and is funded by the US Department of Defense.

Japan

2. The Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) is an independent organization established in 1996. It is a central point for coordinating the activities of experts at sites where security breaches have occurred. While the experts provide technical support to the affected sites, the JPCERT/CC facilitates the cooperation among the experts to solve the security problem at hand. JPCERT/CC does not, however, offer maintenance or consulting service.

Singapore

3. Set up in 1997, the Singapore Computer Emergency Response Team (SingCERT) is funded and driven by the Infocomm Development Authority of Singapore and National University of Singapore. It is a one-stop center for security incident response offering the following services –

- broadcasting alerts, advisories and security patches.
- performing proactive checking or probing of systems and providing tools for intrusion detection.
- promoting security awareness through security courses, seminars and workshops.

- collaborating with vendors or other CERTs to find solutions to security incidents. 98

Canada

4. The Canadian Computer Emergency Response Team (CanCERT) was established by a private firm in 1998 and is recognized by the Government of Canada. In addition to the collection and dissemination of information on computer threats, CanCERT offers security support to its clients for a fee.

Australia

5. The Australian Computer Emergency Response Team (AusCERT) is run by the University of Queensland and it has close ties with the US CERT/CC at Carnegie Mellon, other international CERTs and the Australian Federal Police. AusCERT facilitates communication among affected parties, gives suggestions based on experience and disseminates warnings to other parties who may be at risk.

Annex 9

Publicity and Education Efforts

Hong Kong Police Force

The Crime Prevention Bureau (CPB) and Computer Crime Section (CCS) of the Police have been actively engaged in public awareness and education programs on computer security issues. Frequently, CPB officers give school talks for students, parents or teachers. In addition, upon request, CPB officers visit private businesses and speak to both staff and management about computer security and the development of good security policies. CPB and CCS officers also attend public seminars on general computer security matters. At most major computer related exhibitions held in Hong Kong, CPB operates a booth to promote awareness of computer security. CPB has produced a variety of computer security promotional materials including leaflets, mouse pads, stickers and posters for distribution at public education functions. Computer security information is also available on the CPB website.

2. CPB is planning to work with the Education Department to review the current information technology syllabus and expand the curriculum on subjects dealing with computer security, ethics and moral responsibilities of computer users, as well as a detailed explanation of the laws relating to computer crime. There is also a plan to work with Internet service providers (ISPs) to send warning letters to subscribers who have been identified as abusing their Internet connection. In addition, CPB will work with ISPs to alert broadband service subscribers that they are more at risk from computer security threats due to their static on-line identity.

Information Technology and Broadcasting Bureau (ITBB) and Information Technology Services Department (ITSD)

3. ITBB/ITSD have undertaken and planned for a number of public education programs. The details are set out at **Enclosure A** to this Annex.

Office of the Telecommunications Authority (OFTA)

4. In February 2000, OFTA launched an anti-spamming program jointly with the Hong Kong Internet Service Providers Association (HKISPA) and the Office of the Privacy Commission for Personal Data (PCO). A press release was issued announcing the introduction of an Internet Services Providers Industry Code of Practice to tackle spamming on the Internet. In consultation with HKISPA and PCO, OFTA has prepared and distributed promotional leaflets which contain useful tips for Internet users to minimize the nuisance for receiving spam. Anti-spamming information is offered on OFTA's homepage and promotional leaflets are available from all District Offices and major Post Offices.

5. In April 2000, working in close collaboration with the Consumer Council, OFTA issued a press release alerting the public to the fraudulent practice by some overseas websites which would switch call connections from the Internet to IDD.

Office of Privacy Commission for Personal Data (PCO)

6. In January 1998, PCO published two booklets on personal data privacy on the Internet providing guidance to organizations and individual Internet users respectively. The booklet for organizations seeks to assist website operators to comply with the Personal Data (Privacy) Ordinance (PDPO) in the collection, display and transmission of personal data over the Internet. The booklet for individual users seeks to raise their awareness of privacy risks on the Internet. It gives them guidance on how to protect their personal data privacy by suggesting precautionary actions that can be taken.

7. In February 1999, PCO published a third booklet to provide practical guidance to website operators on compliance matters of the PDPO.

Commerce and Industry Bureau (CIB)/Intellectual Property Department (IPD)

8. IPD is the executive agency in carrying out education work in respect of intellectual property rights protection. Between 1997 and June 2000, IPD delivered talks to 260 secondary schools to arouse the students' awareness of the importance to respect intellectual property rights. The presentations illustrate issues on user licence agreements for computer software, and on the downloading of freeware or shareware from the Internet. IPD also runs talks for other professions, including civil servants, on similar issues.

9. In 1999, IPD organized an international symposium on the inter-linkage between intellectual property and information technology with the Hong Kong Intellectual Property Society.

Hong Kong Productivity Council

10. In addition to those programs which have been undertaken jointly with ITSD (please see Enclosure A), the Hong Kong Productivity Council has provided the following education opportunities to the business community to enhance their knowledge of information security.

(a) An Information Security Seminar for 450 participants was held in November 1999 with speakers from HKPF, HKISPA and HKUST.

(b) Eight training courses on Implementing Internet/Intranet Security were organized for over 550 participants between October 1999 and July 2000.

(c) An e-Cert Promotion and Support Centre was set up jointly with Hong Kong Post in February 2000 to promote the use of e-Cert.

(d) A 3-day event of "Information Security Showcase" was held in April 2000 with 11 organizations displaying their information security services and products to over 4,000 visitors. At the same time, 16 seminars were arranged to increase the visitors' awareness of the issues involved in computer hacking.

(e) The HK e-Award was organized jointly with ITBB in March 2000 to promote the importance of consumer protection on business websites.

(f) A training course for more than 40 participants on public key infrastructure management was organized in March 2000.

(g) Six half-day seminars to promote the use of e-security solutions were held between February and July 2000.

(h) More seminars on information security will be held in September and November 2000.

(i) The education leaflet "Guide to Personal Data Privacy and Consumer Protection on the Internet" was published in April 2000. The project was supported by the Consumer Council and PCO.

Consumer Council

11. In addition to conducting pre-summer vacation school talks on Internet security, the Council has published various articles in its *Choice* magazine since June 1998 covering general and specific Internet topics. They include such items as –

- spamming;
- securities trading on the Internet;
- Internet shopping;
- payment systems in e-commerce;
- Internet Sweeps to identify sites with dubious medical advertisements;
- the IDD trap i.e., problem sites that can redirect a dial-up Internet access connection to an overseas server via IDD;
- consumer data protection in e-commerce; and
- how to establish traders' identity in cyberspace.

Enclosure A to Annex 9

Public Education Activities by ITBB/ITSD

Public Education Programs related to Information Security – Past Activities

No.	Activities	Date	Format/ Frequency	Objective	Target Client
1.	Information Security Seminar (Jointly organised by ITSD and the Hong Kong Productivity Council)	10 Nov 1999	Seminar/ One-off	To promote the awareness of information security.	IT professionals and users. (around 400 participants)
2.	IT Appreciation for Parents programme (Speakers are invited from the Education Department, the Chinese University of Hong Kong and the Hong Kong Police Force)	Launched on 12 Dec 1999 (Post implementation review was conducted in May 2000)	VCD + Leaflets/ during the academic year 1999/2000	To provide IT education for parents so that they can provide necessary guidance to their children on using IT properly. One of the major objectives is to alert the parents to the possible impact and legal concerns of using the Internet.	Parents of the secondary schools. (around 130 secondary schools have participated) (based on the feedback from the secondary schools, project team will work out a different approach to introduce this programme to the parents of primary school students)

No.	Activities	Date	Format/ Frequency	Objective	Target Client
3.	E-commerce Forum for SMEs	8 Mar 2000	Seminar + Mini-exhibition/ One-off	To provide information to the SMEs about e-commerce related services available in the market. Speaker from the HongKong Post was invited to talk about information security and legal issues.	Local SMEs. (around 700 participants)
4.	Cyber-training programme on E-commerce	April 2000	VCD	To promote e-commerce. Public Key Infrastructure (PKI) is one of the topics on the VCD.	General Public. (around 140,000 VCDs were distributed)
5.	Seminar on Security and Hacking (Jointly organised by ITSD and the Hong Kong Computer Society)	1 Apr 2000	Seminar/ One-off	To promote the awareness of Information Security.	IT professionals and users. (around 250 participants)

No.	Activities	Date	Format/ Frequency	Objective	Target Client
6.	Information Security Showcase (Organised by the Hong Kong Productivity Council and supported by ITSD)	12-14 Apr 2000	Seminar + Exhibition/ One-off	To promote the awareness of Information Security and to provide information about the available solutions.	IT professionals and users. (around 4,000 visitors)
7.	Internet Web Page Hosting - Computer Virus - Information Security	April 1999 March 2000	Ongoing	To promote public awareness of information security and computer viruses, and provide guidelines on information security and precaution and alerts on computer viruses.	General Public.
8.	E-commerce in the New Millennium	31 May 2000	Seminar/ One-off	To enhance the awareness and knowledge on e-commerce of the local SMEs. Speaker from the Hongkong Post has been invited to talk about information security and legal issues.	Local SMEs. (around 400 participants)

No.	Activities	Date	Format/ Frequency	Objective	Target Client
9.	Public Key Infrastructure web pages on Digital 21 website (www.digital21.gov.hk)	14 August 2000	Web pages	To provide information about Public Key Infrastructure, Electronic Transactions Ordinance, digital certificates, and other related concepts.	General Public.
10.	Announcement of Public Interest (API) on public key infrastructure (The API was produced by ITBB)	10 Jul 2000	API/ One-off	To promote public key infrastructure and digital certificates for use in secure electronic transactions.	General Public
11.	Internet & Information Security Seminar (Jointly organised by ITSD and the Hong Kong Productivity Council)	12 Jul 2000	Seminar/ One-off	To promote the awareness on information security	IT professionals and users (around 450 participants)
12.	Internet Commerce Expo 2000	27-29 Jul 2000	Exhibition / One-Off	To promote the ESD scheme & related services (such as PKI and awareness on IT security)	IT professionals and public

No.	Activities	Date	Format/ Frequency	Objective	Target Client
13.	Press Conference jointly organised by ITBB and Consumer Council on promoting PKI (ITSD to provide support to ITBB to perform the demonstration)	15 Aug 2000	Press Conference / One-off	To promote PKI and announce the publication of a PKI article in the CHOICE magazine	General Public
14.	Publication of leaflets/pamphlets on Virus Protection	17 Jul 2000	Pamphlets/ One-off	To promote public awareness on virus protection and provide guidelines on best practices in protection computer against virus.	General Public
15.	Publication of an article on PKI in the CHOICE magazine	15 Aug 2000	Article/ One-off	To promote public awareness on PKI.	General Public

Public Education Programs related to Information Security – Planned Activities

No.	Activities	Date	Format/ Frequency	Objective	Target Client
1.	A series of seminars on Information Security (To be jointly organised by ITSD and the Hong Kong Productivity Council)	15 Sep 2000 and 16 Nov 2000	Seminar/ One-off	To promote the awareness on information security	IT professionals and users.
2.	Publication of leaflets/pamphlets on Information Security	Aug 2000	Pamphlets/ One-off	To promote public awareness on information security and provide guidelines on best practices in protection of information security.	General Public
3.	3rd Cycle ESD scheme roving show (Housing Estates)	Mid-Aug to Mid-Sep 2000	Roving Show / One-off (6 locations)	To promote the ESD scheme & related services (such as PKI and awareness on IT security)	General Public
4.	Publication of leaflets/pamphlets on PKI and digital certificates	Sep 2000	Pamphlets/ One-off	To promote PKI and digital certificates	General Public

No.	Activities	Date	Format/ Frequency	Objective	Target Client
5.	Public Key Infrastructure web pages on Digital 21 website (www.digital21.gov.hk)	Sep 2000	Web pages	To enhance the web pages by adding Q&As and an interactive game	General Public
6.	Asian IT Expo 2000	27-30 Sep 2000	Exhibition / One-off	To promote the ESD scheme & related services (such as PKI and awareness on IT security)	General Public
7.	Software Exhibition 2000	15-18 Nov 2000	Exhibition /One-off	To promote the ESD scheme & related services (such as PKI and awareness on IT security)	General Public
8.	4th Cycle ESD scheme roving show (Government Offices)	Mid-Dec 2000 to End-Jan 2001	Roving Show / One-off (6 locations)	To promote the ESD scheme & related services (such as PKI and awareness on IT security)	General Public

Information Technology Services Department
August 2000

Annex 10

Fight Crime Committee (FCC)

Terms of Reference

(1) To draw up plans for a co-ordinated effort to reduce crime.

(2) To co-ordinate the work of the departments and agencies concerned in the implementation of such plans.

(3) To receive and to assess reports from the departments and agencies concerned on the extent to which they have been able to implement the plans and on the results.

(4) To determine ways in which the public can be stimulated to contribute to the reduction of crime.

(5) To receive and to process suggestions from any source on how crime might be reduced.

(6) To recommend any legislative and administrative measures that the Committee considers necessary towards reducing crime.

(7) To report on progress to the Chief Executive once yearly.

Membership (as at August 2000)

Chief Secretary for Administration	(Chairman)
Secretary for Justice	(Deputy Chairman)
Secretary for Security	
Secretary for Home Affairs	
Secretary for Health and Welfare	
Secretary for Education and Manpower	
Commissioner of Police	
Commissioner of Correctional Services	
Dr. the Hon. Rosanna WONG Yick-ming, J.P.	
Mrs. Miriam LAU Kin-yee, J.P.	
Mr. James TO Kun-sun	
Mr. Edward PONG Chong, J.P.	
Mr. Almon POON Chin-hung	
Mr. Raymond CHOW Wai-kam, J.P.	
Professor Daniel SHEK Tan-lei, J.P.	
Mr. CHENG Sing-yip	
Principal Assistance Secretary for Security (E)	(Secretary)

Annex 11

Information Infrastructure Advisory Committee (IIAC)

Terms of Reference

In pursuit of Government's objective to make Hong Kong a leader in the information world of tomorrow, the IIAC will advise Government on the steps to take to facilitate the development of the information infrastructure in Hong Kong. In particular, the IIAC will advise on the policy, regulatory, technical and other related issues in the following areas –

(1) the further development and enhancement of the physical communications infrastructure in Hong Kong;

(2) the development of an open, common interface mounted on established communications network through which individuals, business and government can interact easily and securely using their own systems;

(3) the development of applications which make effective use of the common interface;

(4) the formulation of Hong Kong's position at, and contribution to, international and regional fora on issues relation to the global and regional information infrastructure and electronic commerce; and

(5) the promotion of community awareness and creative use of information technology.

Membership (as at July 2000)

Secretary for Information Technology and Broadcasting (Chairman *ex officio*)

Mr. CHANG Chi-chou

Professor Francis CHIN

Mr. Paul CHOW

Mr. Kenneth FANG, J.P.

Dr. KAN Wing-kay

Professor Charles KAO

Dr. William LO, J.P.

Mr. Dennis LUI

Mr. Charles MOK

Mr. SIN Chung-kai

Mr. Kenneth TING, J.P.

Mr. TSANG Lai-keung

Dr. John URE

Mr. YIP Chee-tim

Mr. Justin YUE

Secretary for Education and Manpower or his representative (*ex officio*)

Secretary for Commerce and Industry or his representative (*ex officio*)

Director-General of Telecommunications or his representative (*ex officio*)

Director of Information Technology Services or his representative (*ex officio*)

Annex 12

Council of Europe's Draft Convention on Cyber-crime*

Checklist

Council of Europe's Draft Convention		Situation in Hong Kong
Article	**Brief Description**	
1	Glossary of terms used in the Convention	Not applicable.
2	Each party to the convention shall create offences for unauthorized access to computer system.	We have the offences of unauthorized access to computer by telecommunication under S. 27A of the Telecommunications Ordinance (Cap. 106) and access to computer with criminal or dishonest intent under S. 161 of the Crimes Ordinance (Cap. 200). The Working Group has recommended to strengthen these offences.
3	Each party to the convention shall create offences for unauthorized and intentional interception of non-public transmissions of computer data.	The Working Group has recommended to clarify the coverage of the current legislative provisions so that all computer data at all stages of storage or transmission will be protected against unauthorized access.
4	Each party to the convention shall create offences for unauthorized and intentional interference of computer data.	This is covered by our offence of criminal damage in S. 60 of the Crimes Ordinance (Cap. 200).
5	Each party to the convention shall create offences for unauthorized and intentional interference of the functioning of a computer system.	Our offence of criminal damage also covers this.
6	Each party to the convention shall create offences for the production, distribution or possession of devices or passwords specifically for the purpose or with intent that they be used for committing offences in Articles 2 to 5.	The Working Group has considered the issue and recommended not to legislate against the possession of hacking tools as there may be legitimate reasons for their existence. We have nonetheless recommended to strengthen our law to protect computer data, including passwords, from being trafficked.

* Version number 19 dated 25 April 2000.

Council of Europe's Draft Convention		Situation in Hong Kong
Article	**Brief Description**	
7	Each party to the convention shall create offences for computer data forgery.	We have the offence of false accounting in S. 19 of Theft Ordinance (Cap. 210) to cover forgery of data for accounting purpose. The offence of criminal damage involving the misuse of computer (S. 60 of Cap. 200) is also relevant.
8	Each party to the convention shall create offences for fraud through manipulating computer data or interference of computer system.	S. 161 of the Crimes Ordinance is relevant – access to computer with criminal or dishonest intent.
9	Each party to the convention shall create offences related to the production, distribution and possession of child pornography through or in a computer system.	The issues are being dealt with by the Prevention of Child Pornography Bill.
10	Each party to the convention shall create offences related to the unauthorized reproduction and distribution by means of a computer system of works protected by copyright, where such acts are committed intentionally on a commercial scale.	This is covered by S. 26 and S. 118 of the Copyright Ordinance (Cap. 528).
11	Each party to the convention shall create offences for attempting and aiding and abetting to commit offences mentioned in Articles 2 to 10.	Attempting, and aiding and abetting the commission of offences are already offences in Hong Kong.
12	Each party to the convention shall provide for corporate liability for offences created under the Convention.	There are similar provisions in Hong Kong.
13	Punishment for the above criminal offences should be effective, proportionate and dissuasive sanctions and measures.	Penalties in our laws are based on similar principles. The Working Group has also proposed improvements in respect of penalties for certain offences to reflect more accurately their seriousness.

Council of Europe's Draft Convention		Situation in Hong Kong
Article	**Brief Description**	
14	Competent authorities are to be empowered to search and seize computer system and data for criminal investigations or proceedings.	Investigation officers can obtain warrants under the relevant legislation to search for and seize evidence.
15	Competent authorities should be empowered to order a person to submit computer data required for criminal investigations and proceedings.	The Production Order under the Organized and Serious Crimes Ordinance (Cap. 455) is relevant. The Working Group has also recommended to adopt compulsory disclosure procedures for encrypted computer data in respect of more serious offences.
16	For the purposes of criminal investigations or proceedings, competent authorities are to be empowered to require a person to preserve specified stored data in the person's control and to keep confidential the undertaking of such preservation.	This may already be done under existing legislative provisions.
17	In pursuance of Article 16, there shall be legislative or other measures to ensure expeditious preservation of traffic data concerning a specific communication.	This may already be done under existing legislative provisions.
18	Under discussion - details not available.	Not applicable.
19	Each party has to establish jurisdiction over offences mentioned in Articles 2 to 11 when the offences are committed within the jurisdiction of the state or by one of its nationals outside its territorial jurisdiction.	The Working Group has already looked into the jurisdictional problem and made recommendations enabling Hong Kong courts to have jurisdiction over the offence if the person who obtains access to a computer is in Hong Kong or the computer to which access is obtained is in Hong Kong.

Council of Europe's Draft Convention		Situation in Hong Kong
Article	**Brief Description**	
20	Parties to the convention have to provide each other assistance in the investigation of computer related offences and for the collection of electronic evidence of a criminal offence.	We respond positively to calls for assistance from our counterparts from outside Hong Kong.
21	The criminal offence established in accordance with Articles 3-5 and 7-11 shall be extraditable offences between or among parties to the Convention.	The offences described in Schedule 1 of the Fugitive Offenders Ordinance (Cap. 503) are extraditable offences. They include *mischief in relation to computer data* and *offences involving the unlawful use of computers*.
22	Parties to the convention are to afford one another mutual assistance to the widest extent possible for the purpose of investigations and proceedings concerning computer related offence or for the collection of electronic evidence of a criminal offence.	This is observed where mutual legal assistance agreements exist with other jurisdictions.
23	Each party to the convention shall set down procedures pertaining to mutual assistance requests where there is no mutual assistance treaty or agreement.	The proposal is in line with our present practice.
24	A party to the convention shall take all appropriate measures to preserve expeditiously the specified data upon request by another party. For the purpose of responding to a request, dual criminality shall not be required as a condition to providing such preservation, but may be required as a condition for the disclosure of the data to the requesting party.	The absence of dual criminality elements means that the alleged activities may not be an offence in Hong Kong. If that is the case, it will be almost impossible to get a warrant or court order to preserve the data. It appears that it is futile to attempt to preserve the data in such cases. Nonetheless, the general thrust that data should be preserved as expeditiously as possible is also our goal.

Council of Europe's Draft Convention		Situation in Hong Kong
Article	**Brief Description**	
25	When in the course of execution of a request under Article 24, the requested party discovers that a service provider in a third state was involved in the transmission of the communication, the requested party shall expeditiously disclose to the requesting party a sufficient amount of traffic data in order to identify that service provider and the path through which the communication was transmitted.	This is in line with our present practice.
26	Upon request by another party to search, seize or secure data stored by means of a computer system, the requested party shall execute the request as expeditiously as possible.	This is in line with our present practice.
27	A party may obtain data in another jurisdiction if the data are publicly available or the data subject has given consent for the party to access the data.	This is in line with our present practice.
28	Under discussion – details not available.	Not applicable.
29	Each party shall designate a point of contact available on 24-hour, 7-day per week basis to ensure the immediate assistance to other member states in - (a) providing technical advice; (b) preserving data expeditiously; and (c) collection of evidence, giving of legal information and locating of suspects.	This will be an internal arrangement among Council of Europe member states. Nonetheless, we should explore if Hong Kong may join similar efforts if they are not limited to sovereign states.