**BY FAX AND BY POST**
**(2521 2848)**

Our Ref.: C/ITC(8), M1945 16 March 2001

Ms. Cheung Siu-hing
Deputy Secretary for Security,
Security Bureau,
The Government of the Hong Kong
Special Administrative Region,
Lower Albert Road,
Central, Hong Kong.

Dear

**Report on the Inter-departmental Working Group on Computer Related Crime**

--- I have pleasure to enclose a copy of the joint submission of the Society and the Information Systems Audit and Control Association (Hong Kong Chapter) on computer-related crime for your consideration.

With best regards.

Yours sincerely,

LEE KAI-FAT
REGISTRAR
HONG KONG SOCIETY OF ACCOUNTANTS

KFL/ay
Encl.

**Hong Kong Society of Accountants (HKSA)**
**and**
**Information Systems Audit and Control Association (ISACA)**

**BY FAX AND BY POST**
**(2521 2848)**

Our Ref.: C/ITC(8), M1945 16 March 2001

Mr. John Lee,
Security Bureau,
Government Secretariat,
Lower Albert Road,
Hong Kong.

Dear Mr. Lee,

**Report on the Inter-departmental Working Group on Computer Related Crime**

--- Please find attached a joint submission on the above-referenced report from the Hong Kong Society of Accountants (HKSA) and the Information Systems Audit and Control Association (ISACA) (Hong Kong Chapter).

We hope that you will find our comments to be helpful.

LEE KAI-FAT
REGISTRAR
HKSA

PIERRE HERBST
PRESIDENT
ISACA (HK CHAPTER)

**HONG KONG SOCIETY OF ACCOUNTANTS (HKSA)**

**AND**

**INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA) HONG KONG**

# JOINT SUBMISSION TO SECURITY BUREAU

## RE: Inter-Departmental Working Group Report on Computer Related Crime

The Hong Kong Society of Accountants ("HKSA") and the Hong Kong Chapter of the Information Systems Audit and Control Association ("ISACA") have pleasure in submitting the following comments to the Security Bureau on the Report by the Inter-Departmental Working Group on Computer Related Crime ("the Report").

We recognise the increasing need to address the issue of computer related crime, particularly given the fast pace of development in information technology and the continued growth in electronic commerce.

We therefore welcome the initiative by the Government of the Hong Kong Special Administrative Region ("the Government") to strengthen the overall framework that deals with the challenges relating to the prevention of, and the fight against, computer related crime.

We commend the Inter-Departmental Working Group ("the Working Group") on a thorough and balanced report that addresses not only the law enforcement aspects but also general awareness on computer security and related areas. We support the efforts by the Working Group as part of the Government overall initiatives in combating computer related crime.

In this submission, we seek to address specific issues discussed in the Report as well as the recommendations made by the Working Group. Our comments seek to focus on the practical aspects, as seen from our viewpoint as professional advisors.

### The Role of the Government in Combating Computer Related Crime

Considering the time needed to effect legislative changes, the legal framework will inevitably lag behind the pace of technological changes. As such, it would not be practical to rely entirely on the Government to lead efforts in combating computer related crime, nor to rely solely on the legal framework as the only means of protecting the public against such crimes.

We therefore strongly support the Working Group's emphasis on public awareness and education. We believe that the Government should also take the role of a facilitator, focusing on the setting of policies and principles and, where appropriate, takes the lead in the adoption of good practices and industry standards.

Furthermore, the introduction of legislation would assume that a consensus has been achieved as to where the balance should lie between the prevention and detection of computer fraud and the safeguarding of personal liberties and privacy. It is not clear that such a consensus currently exists and, given the sensitivity of this issue, it would be desirable for there to be wider debate on it within the community before any detailed proposals for major legislative changes are formulated.

**Existing Legislation (Chapter II)**

*As long as the intention and substance of the proposed changes are clear, it will be left to the law draftsman to decide on the most appropriate legislative vehicle for effecting the proposed changes (para. 2.8).*

In conjunction with the drafting of any detailed legislative proposals to give effect to the recommendations in the Report, it would be desirable to carry out a review of the whole body of legislation on which such proposals may impinge to ensure that there are no conflicts of approach amongst the different ordinances. This may be particularly important if it is decided to effect the changes in one ordinance.

**Meaning of the Term "Computer" (Chapter III)**

*The term "information system" as defined in the Electronic Transactions Ordinance (Cap. 553) should be used in place of "computer" (paragraph 3.9).*

We appreciate the difficulties surrounding the interpretation of the term "computer". "Computer" tends to imply the tangible elements, such as hardware, software, network components, etc. "Information system", on the other hand, has a broader meaning, encompassing not just the technical components, but also the data, information and even related processes (which could be manual) that together make up a functional system, which captures, processes, analyses and disseminates information to users of the system.

Given this much broader interpretation of "information system", which often depends on the context within which it is used, we are not entirely convinced of the merits of using it to replace the term "computer". We would suggest that consideration be given instead to making reference to the term "information system" within the definition of "computer".

**Jurisdiction (Chapter IV)**

*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 (para. 4.10).*

We appreciate the need for this study, and concur that the specific offences proposed to be brought under the Ordinance would enable the courts to more effectively deal with computer crime.

However, we would urge great caution in any amendment to the Criminal Jurisdiction Ordinance; we concur with the view of the Working Group that such amendments should not be attempted lightly.

**Encryption (Chapter V)**

*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 (para. 5.14).*

*The compulsory disclosure requirement should be subject to judicial scrutiny ... the disclosure power should apply to offences of a more serious nature ... 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 (paras. 5.18, 5.25-5.26).*

We are aware of the need for some form of compulsory disclosure requirements in relation to cryptographic keys and tools given that these are used increasingly by organisations to safeguard critical information. However, it is important to study such requirements in detail such that a balanced approach can be agreed by all stakeholders (the Government, law enforcement, industry, etc.).

With regard to the recommendations, which refer to both decryption tool and decryption keys, we wish to point out that, in all likelihood, most organisations would make use of proven encryption/decryption tools, the source codes of which should be readily available. In our view, legislative focus should be on keys rather than the actual cryptographic tools.

The Bureau needs to recognise that the disclosure of encryption/decryption keys remains a sensitive issue and, based on experience at other jurisdictions, is one that is likely to be met with the most resistance.

We would advise against the establishment of a mandatory key escrow scheme. Apart from establishing sufficient safeguards in respect of such powers, such as the suggestions to limit this to serious offences, it is also important to protect the confidentiality of the information obtained in the process, particularly in respect of the cryptographic keys.

As regards limiting the disclosure power to "offences of a more serious nature", it is debatable whether the proposed threshold of offences carrying a maximum penalty of not less than 2 years' imprisonment is sufficiently high. The Working Group's report itself recommends maximum penalties of 5-10 years or more for serious offences (see e.g. paras. 6.22, 7.11). Under the Companies Ordinance, for example, various offences that are primarily of a regulatory nature provide, on indictment, for a maximum sentence of 2 years' imprisonment upon conviction. Under the circumstances, "not less than 5 years" might be a more realistic threshold.

**Protection of Computer Data (Chapter VI)**

*Unauthorized access by any means, e.g., through a "stolen" password with or without the use of telecommunication, should also be made unlawful (para. 6.19)*

The Report tends to concentrate on incidents of "external" fraud and addresses issues relating to "unauthorised access". It is not clear that this term will cover cases involving unauthorised access to data and information by an organisation's own employees. This type of potential situation also needs to be studied and recommendations made if the various possible electronic security risks are to be fully addressed.

Where new offences are created, it will be essential to consider the potential ramifications from a law enforcement viewpoint. As technology advances, situations may be created that cause potential enforcement issues where these were not intended. For example, there exist automated tools that collect information when loaded on target systems. Such tools can be used for genuine purposes, such as to collect useful information for providing system support, marketing or to support decision making. These tools can also be used in a malicious manner, such as to collect certain information and transmit these to the perpetrator of an intended offence. The law would need to differentiate between, for example, a person using such tools to advance his/her own interest; a company using such tools to collect marketing information without the knowledge of their customers; and the legitimate use of such tools.

Paragraph 6.19(a) further recommended the clarification of "data" to include all data transmitted or being transmitted "via a computer or the Internet". We believe specific reference to "computer" or "Internet" may be unnecessary, as the transmission means/medium should be kept to a general level.

*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 ... We recommend that the proposal should not be pursued (para. 6.23).*

We support the recommendation in paragraph 6.23 regarding hacking tools. These tools are often legitimately applied by security specialists and system managers to test and/or determine the vulnerability of their computer networks and systems.

**Penalties for Offences: Jurisdiction (Chapter IV); Protection of Computer Data (Chapter VI); "Deception" of Computers (Chapter VII)**

*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 (para. 4.16).*

While in principle it is reasonable to have regard to the offence intended to be committed when considering the penalty for unauthorised access with intent, presumably the penalty should be generally be commensurate with the penalties for the offences of "attempted 'x'" rather than the actual offences of "x".

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

While the effect of unauthorised access to a computer may be "akin" to theft, we should not lose sight of the important potential differences. If it is proposed to follow the model of section 27A of the Telecommunications Ordinance, then no element of dishonesty needs to be proved (see para. 6.18), unlike with the offence of theft. This needs to be borne in mind when considering the appropriate penalty for unauthorised access.

*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 (para. 7.11).*

This is reasonable.

**Assistance from Internet Service Providers (ISPs) (Chapter VIII)**

*... 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 (para.8.16).*

Currently certain industries, such as banking, have well documented policies and procedures requiring organisations operating in that field to "know their customers". Often this implies the use of strong authentication, usually face-to-face authentication, at the point when a customer opens an account with a financial institution.

Paragraph 8.14 seems to suggest that ISPs should also be required to obtain positive proof of a subscriber's identity. In Hong Kong, this inevitably means the capture and storage of a person's Hong Kong Identity Card details.

We would urge caution in relation to this suggestion, regardless of the fact that such requirements will need to conform to the requirements set out in the Personal Data (Privacy) Ordinance. Further, for organisations that wish to establish Internet access on behalf of their staff / members, such as schools, companies, etc., it is important to establish the impact of such requirements on the organisations' internal procedures on registering its own users.

*ISPs should be encouraged to keep log records including the calling numbers as a good management practice ... administrative guidelines on record-keeping by ISPs should be drawn up ... (paras. 8.24, 8.26).*

The Working Group recommends that ISPs be encouraged to retain log records for a reasonable period of time, such as six months. Whether or not six months is in practice a reasonable period of time depends on the volume of traffic on the Internet, which is increasing all the time. This area would require further consideration to avoid such requirements being a burden to the service providers.

*Consumers should be encouraged to choose ISPs who adopt the good management practices set out in these [industry] guidelines ... (para. 8.27). Internet users should be encouraged to make use of the Public Key Infrastructure for enhanced security, although the requirement should not be made mandatory (para. 8.23).*

Consumer awareness would be the key to success. This is a significant undertaking given that the average consumer has a limited awareness of such matters, as well as of technologies such as PKI. Direction should be given on the standards of such guidelines, and on the business practices that should be adopted by the service providers.

*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 (para. 8.30).*

In view of the volume of information, and the borderless nature of the Internet, we do not feel that it is practical to implement such proposals. Further, the blocking of such services is also not practical, particularly since a user can dial up to overseas ISPs who are not subject to such requirements.

**Protection of Critical Infrastructures (Chapter IX)**

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

*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. 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 (para. 9.17).*

We strongly support this view. However since a lot of the systems are inter-connected, it would not be sufficient to just focus such efforts on specific sites: security is only as strong as the weakest link. A coordinated effort to enhance the overall security would be required. The success in the efforts to address the Year 2000 issue would be a good example to follow.

It would also be worthwhile to consider the questions of whether and how to promulgate guidance on minimum standards of computer security for critical infrastructures. It would probably be more appropriate for any such guidance to focus more on principles rather than technical specifications given the differences between the various sectors that would be affected.

**Public Education (Chapter X)**

*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 (para. 10.7).*

We strongly agree with this recommendation. Awareness is central to enhancing the overall framework on information security. As two of the key professional associations in Hong Kong, we are committed to improving our members' awareness through continuing professional education and are willing to lend support to this initiative insofar as we can.

We believe that the Government, in particular the Education Department and Universities, should consider including subjects such as IT/IS control, security, ethics, etc., into the current curriculum. For example, the Information System Audit and Control Association ("ISACA") published a set of "Model Curricula for Information Systems Auditing at the Undergraduate

and Graduate Levels". We would urge the Government to consider integrating such framework within the education system as soon as practically possible.

**The Private Sector's Role (Chapter XI)**

*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 (para. 11.12).*

There already exist a number of such standards and schemes in relation to information security. Two of the more prominent standards/schemes are:

- WebTrust Principles and Criteria - an initiative to provide independent third party assurance, spearheaded by the accounting institutes in US and Canada, and taken up in Hong Kong by the Hong Kong Society of Accountants ("HKSA");

- BS 7799 - the standard on Information Security Management developed initially by the British Standards Institution and is due to be published as an international standard by the ISO (ISO/IEC DIS 17799-1).

We would urge the Government to actively explore opportunities to promote or adopt such schemes for Hong Kong.

We believe that strong information security is part and parcel of good corporate governance and both the private sector and the Government should participate in promoting it as such. The HKSA and ISACA (HK Chapter) are certainly willing to participate in relation to this aspect.

**Resources and Capabilities (Chapter XII)**

*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 (para. 12.18).*

The feasibility for such cooperation would depend on the setting up of a standard set of procedures, such as those for handling computer evidence. Without such formal framework, it would be difficult to maintain quality, which may jeopardise the use of computer evidence. We would recommend priority should be given to the development of such standards, with input from interested parties. Members of both the HKSA and ISACA HK are exploring this particular area, and will be happy to contribute to such efforts.

**Future Institutional Arrangements (Chapter XIII)**

*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 (para. 13.8).*

*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.) (para. 13.9).*

The fast pace of development in information technology and its application is likely to demand a more permanent mechanism to be established by the Government to review, on a more regular basis, opportunities in enhancing the overall framework in areas relating to information technology, including but not limited to those relating to the combat of computer related crime. We therefore support the recommendation to establish a mechanism to keep track of such matters.

However, given the issues do not relate entirely to law enforcement, we believe that the focus should not be just limited to addressing computer crime. Equal emphasis should be given to education, building security awareness, etc. We therefore believe that when deciding the composition of the sub-committee and private sector representation, this particular aspect should be considered.

HKSA and ISACA (HK Chapter)

March 15, 2001