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

BY FAX AND BY POST
(2877 8024)

Our Ref.: C/COG, M0909

6 February 2001

Mr. Raymond Lam,
Clerk to LegCo Panel on Security,
Legislative Council Secretariat,
3rd Floor, Citibank Tower,
3 Garden Road,
Central,
Hong Kong.

Dear Mr. Lam,

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

--- We attach for the purposes of the meeting of the Panel of Security on 10 February 2001, a joint submission on the above Report from the Hong Kong Society of Accountants (HKSA) and the Information Systems Audit and Control Association (ISACA).

As previously indicated, the following representatives from the respective organisations will be attending the meeting:

HKSA	Mr. Michael Chan Mr. Peter Tisman
ISACA	Ms. Susanna Chiu Mr. William Gee

As this is a joint submission, it would be helpful if you would arrange the four representatives to sit together in the Legislative Council Meeting.

WINNIE CHEUNG
DIRECTOR OF PROFESSIONAL PRACTICES
HKSA

SUSANNA CHIU
VICE PRESIDENT
ISACA (HK CHAPTER)

Hong Kong Society of Accountants (HKSA)

and

Information Systems Audit and Control Association (ISACA)

JOINT SUBMISSION TO LEGCO PANEL ON SECURITY

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

We have pleasure in submitting the following comments on the Report by the Inter-Departmental Working Group on Computer Related Crime.

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 ("the Report") on the subject.

In this submission, we have outlined our comments only on a number of significant issues discussed in the report. We plan to provide a more detailed submission to the Security Bureau as part of the consultation process.

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 will no conflicts of approach amongst the different ordinances. This may be particularly important if it 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 that captures, processes, analyses and provides information to its users.

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 - which are readily available. Any legislation aimed at securing access to proprietary encryption/decryption tools would be unlikely to be effective. In our view, the focus should be on keys rather than the actual cryptographic tools.

However, the disclosure of encryption/decryption keys remains a sensitive issue, and is one that is met with the most resistance (based on experience at other jurisdictions). 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 “external” fraud and addresses issues relating to “unauthorised access”. It is not clear that this term will cover cases of authorised access involving an unauthorised use. This type of potential situation also need to be studied and recommendations made if the various possible systemic security risks are to be fully addressed.

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)

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 may require further consideration.

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.

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 are concerned with the practical implications of such measures.

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.

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 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.

HKSA and ISACA (HK Chapter)

6th February 2001