Annex

Progress of implementation of recommendations of Inter-departmental Working Group on Computer Related Crime

Working Group's Recommendations*	Lead Action Party	Action	Progress
(A) Short term			
28. Promoting the denial of multiple log-in.	Office of the Telecommunications Authority (OFTA)	Write to Internet Service Providers (ISPs) for cooperation. Promote consumer awareness in this regard.	OFTA has discussed the implementation of this recommendation with the Hong Kong Internet Service Providers Association (HKISPA) and Consumer Council, both of which consider that "multiple log-in" is a neutral function. Instead of deleting this function, it would be more appropriate to make consumers aware of the implications of multiple log-in on computer security. The Consumer Council considers that security awareness of consumers when using ISPs' services should be more widely promoted. The Consumer Council published articles on cyber security in the April 2002 issue of its monthly magazine "Choice". OFTA has also invited HKISPA to enlist its members' help in promoting cyber security awareness among users.

* The numbering corresponds to that used in the Summary of Recommendations in the Working Group's report.

Working Group's Recommendations*	Lead Action Party	Action	Progress
30. Increasing communication between law enforcement and ISPs.	Police	Establish forum for exchange between law enforcement and communication service providers.	To strengthen their communication with ISPs, law enforcement agencies (LEAs) have established a 24-hour liaison system with the major ISPs and other institutions (such as financial institutions). ISPs have designated staff members to maintain close contact with LEAs to deal with contingencies. In November 2003, LEAs held an exchange forum with ISPs to discuss in-depth issues involved in investigating computer offences, the purpose of which was to enhance communication and establish closer cooperation.
39. Stepping up information sharing between law enforcement and private sector.	Police	Include requirement in law enforcement agencies' standard procedures. Invite ideas from private sector on possible additional measures to foster information sharing.	As mentioned above, LEAs have established a 24-hour liaison system with the major ISPs and other institutions (such as financial institutions) to deal with contingencies. In October 2003, the Police conducted a computer security course for financial institutions to enhance the industry's knowledge in computer and cyber security and to promote information exchange.
48 – 49. Continuing and deepening inter-agency cooperation locally and internationally.	Police	Draw up standard procedures to facilitate cooperation and information sharing.	LEAs have been holding regular joint meetings to exchange experience and information. They have also established specific liaison channels with the Hong Kong Computer

Working Group's Recommendations*	Lead Action Party	Action	Progress
			Emergency Response Team Coordination Centre (HKCERT) and other relevant departments to strengthen the coordination and response to information security incidents. As regards cooperation with overseas agencies, local LEAs have compiled a list of overseas LEAs with which they have maintained regular contacts, and will cooperate and liaise with overseas LEAs based on operational needs. The effectiveness of the existing liaison channels with overseas agencies will be reviewed at the joint meetings. Visits will be made to overseas LEAs, and overseas delegations will be received with a view to stepping up communication and cooperation.
(B) Short to medium term			
1. Defining "computer" in law.	Security Bureau (SB)	Prepare draft legislation.	Proposed legislative amendments are being prepared.
3. Including specified offences under Criminal Jurisdiction Ordinance.	SB	Prepare draft legislation.	The draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002 was submitted to the Legislative Council (LegCo) in November 2002. LegCo has set up a subcommittee to scrutinize the draft

Working Group's Recommendations*	Lead Action Party	Action	Progress
			Order.
9 – 14, 16. Improving existing legislative provisions to remove ambiguity, better protect against unauthorized access and prevent trafficking in passwords etc.	SB	Prepare draft legislation.	Proposed legislative amendments are being prepared.
18 – 20. Rationalizing penalties for specified computer offences.	SB	Prepare draft legislation.	Proposed legislative amendments are being prepared.
22 – 25. Drawing up administrative guidelines on record keeping.	Police	Set up forum for drawing up administrative guidelines. Publicize guidelines when available.	LEAs will continue to maintain close liaison with ISPs' cooperation in investigating computer and cyber crimes.
31. Undertaking thorough risk assessment of critical infrastructures.	Commerce, Industry and Technology Bureau (CITB)	Identify critical infrastructures to be covered, draw up steps for conducting the risk assessment.	CITB and the Information Technology Services Department (ITSD) have examined information on how overseas governments determine critical infrastructures and conduct risk assessment. They are now drawing up the criteria for determining critical infrastructures in Hong Kong and preparing preliminary draft guidelines on risk assessment procedures.
37. Introducing mechanism for information sharing, facilitating cross-agency participation,	ITSD	Draw up functions, structure and mode of operation of mechanism.	ITSD has set up an inter-departmental coordination group to facilitate sharing and exchange of information on

Working Group's Recommendations*	Lead Action Party	Action	Progress
mapping out overall public sector education strategy on computer crime.			computer and cyber security as well as prevention of computer crimes; and to strengthen inter-departmental cooperation and liaison on public education. ITSD has also set up a portal website on information security (www.infosec.gov.hk) to provide, on a one-stop basis, information on such issues as computer and cyber security and prevention of computer crimes, so as to supply enterprises and the public with different types of information relating to information security. In addition, ITSD has produced publicity materials (such as posters and leaflets) for distribution to government departments, District Offices, community facilities, community cyber centres, public libraries and schools, for public reference. Stalls are set up at relevant exhibitions from time to time to step up publicity. In 2003 to 2004, ITSD has produced a series of radio and television episodes to more widely promote public awareness of computer and cyber security.

Working Group's Recommendations*	Lead Action Party	Action	Progress
40 – 43. Encouraging private sector to share information and undertake education efforts; increasing public-private sector collaboration.	ITSD	Include message in Government publicity programs, probably in conjunction with item 37.	As mentioned above, ITSD has set up a portal website on information security to provide, on a one-stop basis, information on such issues as computer and cyber security and prevention of computer crimes. ITSD has also liaised with relevant public and private organizations such as the Police, Education and Manpower Bureau (EMB), Television and Entertainment Licensing Authority (TELA), Hong Kong Monetary Authority, Hong Kong Computer Society, Hong Kong Productivity Council and HKCERT, to assist in enhancing and enriching the content of the website.

Working Group's Recommendations*	Lead Action Party	Action	Progress
		Invite major professional organizations and business associations to contribute.	Government departments have collaborated with different public and private organizations from time to time to promote public education on computer and cyber security as well as prevention of computer crimes. Examples are talks on information security organized for private organizations and seminars jointly held with private organizations. ITSD, the Police and HKCERT have jointly produced information security handbooks for small and medium enterprises as well as the general public. EMB in coordination with a number of Government departments and relevant organizations has established a thematic website called "Cyber Ethics for Students and Youth" (cesy.qed.hkedcity.net) to provide suggestions and guidelines on the correct use of computers and the Internet for school, parents and students, and to supply teachers with teaching resources on designing and drawing up relevant syllabuses. In addition, TELA has organized such publicity and public education activities as "Ten Healthy Websites Contest" and "Creating a Healthy Cyber World" to educate children and youngsters on the correct use of the Internet.

Working Group's Recommendations*	Lead Action Party	Action	Progress
54 – 55. Setting up a committee on computer crime with representatives from law enforcement and private sector.	SB	Examine the functions, structure and mode of operation of the committee.	SB is drawing up the terms of reference of the committee. Members will include representatives from the relevant Bureaux, LEAs and private sector.
(C) Medium term			
27. Exploring feasibility of take-down procedures.	Individual Bureaux	Examine and, if possible, adopt in individual policy context.	The procedures will be adopted by individual Bureaux in the light of their overall policy considerations.
31. Undertaking thorough risk assessment of critical infrastructures.	Relevant authorities of individual infrastructures	Conduct assessment.	Assessment will be conducted after the criteria for determining critical infrastructures and guidelines for risk assessment procedures have been formulated.
32 – 33. Establishing mechanism to coordinate preparation and synchronization of protection and recovery plans; including cyber attacks on critical infrastructures in Emergency Response System (ERS).	CITB in initial stage	Having regard to results from item 31, draw up functions, structure and mode of operation of mechanism, and determine relationship between mechanism and ERS.	CITB and ITSD are examining the mechanisms and practices adopted by other countries.

Working Group's Recommendations*	Lead Action Party	Action	Progress
44. Exploring feasibility of audit mechanism to certify information security standards.	SB	Invite major professional organizations and business associations to take the lead in setting industry-specific standards. To facilitate and support as necessary.	SB has written to professional organizations and business associations to invite their consideration of formulating information security standards specifically tailored for the industries under their purview.
50 – 52. Working out standard procedures for handling computer evidence and promulgating them.	Police	Develop common standard. Promulgate standard once available.	The Police have drawn up a computer forensics handbook on the standard procedure for handling computer evidence for use by investigators and computer forensics officers. The handbook has been circulated to other LEAs for reference. LEAs will have further discussions on the development of a common standard.
54 – 55. Setting up a committee on computer crime with representatives from law enforcement and private sector.		Set up committee.	Please refer to the progress of this item on P.8.
(D) Medium to long term			
4 – 8. Mandating disclosure of decrypted text or decryption tool of encoded computer information for investigation, subject to judicial scrutiny and other safeguards.	SB	Work out proposed implementation details and further consult before draft legislation is prepared.	SB is examining the relevant legislation and measures of other countries, and will draw up proposals for consultation.

Working Group's Recommendations*	Lead Action Party	Action	Progress
(E) Long term			
2. Conducting in-depth study of jurisdictional rules.	Department of Justice (D of J)	Conduct study on legal issues involved.	D of J has examined the Criminal Jurisdiction Ordinance. Its view is that the Ordinance is meant to provide exceptions to the normal jurisdictional rules. Changing the ambit of the Ordinance fundamentally to cover all criminal offences should not be attempted lightly. Regarding the deception offences covered by the Ordinance, they often involve the use of computers either as a tool or a storage medium for information. The Ordinance should therefore be sufficient to deal with these offences.
17. Rectifying the gap in law regarding "deception" machines.	D of J	Conduct study on legal issues involved.	D of J has examined the issue of "deception" of machines. Its view is that as many machines nowadays have built-in computers, "deception" of machines could be dealt with by the computer offences under sections 60 and 161 of the Crimes Ordinance. There is therefore no need to effect any legislative amendments at present.
53. Establishing central computer forensic examination unit in the long run	Police	Consider merging existing computer forensic capabilities among law enforcement agencies.	LEAs have conducted preliminary discussions on the establishment of a central computer forensic examination unit, and will further research into this

Working Group's Recommendations*	Lead Action Party	Action	Progress
			issue.