Ref. : SBCR 14/3231/88 Pt. 14

LEGISLATIVE COUNCIL BRIEF

INTER-DEPARTMENTAL WORKING GROUP ON COMPUTER RELATED CRIME : REPORT AND RECOMMENDATIONS

INTRODUCTION

At the meeting of the Executive Council on 21 November 2000, the Council noted the recommendations of the report of the Inter-departmental Working Group on Computer Related Crime (the Working Group).

BACKGROUND

The Working Group

2. The phenomenal increase in computer use over the past few years has been accompanied by an increase in computer-related crimes as well. We therefore established the Working Group in March 2000 to examine existing legislation and related issues regarding computer crime. It was chaired by the Security Bureau and comprised members from other relevant policy bureaux and departments, including the law enforcement agencies.

3. The Working Group's focus was strengthening the framework or environment within which law enforcement against computer crime might be carried out. It therefore sought to identify problems and recommend solutions, legislative or otherwise, regarding crime prevention, evidence gathering, investigation and prosecution arising from computer crime. The aim was to contribute to the total effort of providing an environment conducive to the legitimate use of the computer and the Internet. Given this macro approach, the Working Group did not attempt to deal with each and every offence that might be committed via the computer or the Internet but rather to identify solutions that might be applied across the board.

4. In making its recommendations, the Working Group sought to balance law enforcement facilitation on the one hand against the likely cost of compliance on the other hand. The feasibility of administrative measures instead of legislation and the need for sufficient safeguards to go with proposed additional legislative powers formed an integral part of the Working Group's consideration. As the Internet knows no borders, the Working Group also took into account relevant international developments and trends in its deliberations.

5. The Working Group has covered the following main issues –

(a) whether existing criminal offences and penalties pertaining to computer related crime carry sufficient deterrent effect;

(b) the jurisdictional problem presented by computer crime, which knows no borders;

(c) how law enforcement agencies may obtain access to encrypted computer evidence;

(d) the protection of computer data and passwords from unauthorized access and trafficking;

(e) the protection of critical infrastructures from cyber attacks;

(f) the resources and capabilities of law enforcement agencies in dealing with computer crime;

(g) the assistance which may be rendered by the private sector, including Internet service providers (ISPs), in fighting computer crime;

(h) how existing public education efforts to prevent computer crime may be strengthened; and

(i) what institutional arrangements within the Government are necessary to monitor computer crime issues.

6. The Working Group submitted its report, at the **Annex**, in September 2000. The summary of recommendations is on pages i – viii of the report.

The Findings

7. The Working Group found that the thrust of our existing legislation on computer crime is largely along the right lines. However, there is room for improvement to cater for the following –

(a) some inconsistency in treatment between crimes of similar nature in the physical and cyber worlds; and

(b) the apparent inability of certain legal concepts to catch up with the information age.

8. Very briefly, the Working Group has recommended the following legislative changes –

(a) strengthening and rationalizing the penalties for certain computer offences such as hacking;

(b) extending the coverage of protected computer data (from programs and data stored in a computer to programs and data at all stages of storage or transmission, and from unauthorized access by telecommunications only to unauthorized access by any means);

(c) prohibiting the trafficking of data obtained through unauthorized access to computer;

(d) prohibiting the making available of computer passwords or access codes for wrongful gain, an unlawful purpose or causing wrongful loss to another;

(e) better defining the term “computer” legally;

(f) applying extended jurisdictional rules to certain computer offences; and

(g) requiring the compulsory disclosure of the decryption tools or decrypted text of encoded computer records for more serious offences.

9. Most of the Working Group’s legislative proposals are built on existing legislation. For example, the Working Group has recommended bringing the penalty for the offence of accessing a computer with a dishonest intent to deceive (currently five years’ imprisonment) on par with that for deception offences in general (ten to 14 years). Another example relates to the proposed compulsory disclosure of the decrypted text or decryption key

(para. 8(g) above). There are already provisions in some ordinances for computer records to be produced in a “visible and legible form”. The Working Group’s proposal aims at –

(a) putting beyond doubt that what is required is the plain text and images (or even sounds), and not meaningless codes (which might be argued to be “visible and legible”);

(b) applying the disclosure requirement to all more serious offences meeting an objective criterion, e.g., those offences attracting a maximum sentence of no less than two years’ imprisonment on conviction; and

(c) introducing appropriate safeguards, in particular a judicial scrutiny procedure, to prevent possible abuse.

10. The Working Group emphasized that it will not be enough to rely on legislation alone to combat computer crime. Its report has therefore devoted considerable coverage to administrative measures. Very briefly, these are –

(a) working out an administrative guideline for ISPs regarding Internet account subscriber and log record details to be kept, as well as the period for which such records should be kept;

(b) establishing a regular forum of exchange between ISPs and law enforcement agencies, and a contact point system for ISPs and law enforcement agencies for computer crime investigations;

(c) examining the feasibility of putting in place “take down” procedures for ISPs to remove offending materials or sites in respect of, for example, pornographic materials;

(d) conducting a thorough risk assessment of our critical infrastructures in respect of cyber attacks, and establishing a mechanism for overseeing the preparation and coordination of protection, contingency and recovery plans against computer and Internet-related security threats for these infrastructures;

(e) increasing inter-agency cooperation and sharing of intelligence and experience in respect of computer crime;

(f) stepping up liaison with law enforcement agencies in other jurisdictions to combat computer crime;

(g) developing a common standard for handling computer evidence among all local law enforcement agencies;

(h) establishing a mechanism to facilitate multi-agency participation in and better coordination of publicity and education efforts on computer crime;

(i) increasing the involvement of the private sector in preventing and combating computer crime; and

(j) establishing a sub-committee under the Fight Crime Committee to oversee follow up work of the Working Group's recommendations and monitor evolving developments.

Way Forward

11. The Working Group has outlined a framework within which more detailed work and, in many cases, sustained effort will be required to deal with computer crime. Our initial assessment is that the general thrust of the report appears to be along the right lines. Nonetheless, the growth in the use of information technology means that computer crime issues increasingly impact on society at large. Before coming to a firm view on whether to accept the Working Group's recommendations, therefore, we would like to seek the public's views on the issues raised and the recommendations made in the report. We will therefore release the report for public consultation for a period of two months from 1 December 2000. The feedback received will be taken into account in our detailed assessment as to which recommendations should be accepted and the priorities in implementing them.

FINANCIAL AND STAFFING IMPLICATIONS

12. The majority of the Working Group's recommendations regarding legislative changes may be implemented without significant financial and staffing implications. The preparation of the draft legislation will be absorbed by existing resources. The financial and staffing implications of implementing other recommendations such as those aimed at enhancing the effectiveness of our education efforts, better protecting our critical infrastructures and strengthening existing institutional arrangements will need to be assessed after the detailed arrangements have been worked out. They are however unlikely to be substantial. Should there be any additional resource requirement, we will secure it in the normal manner.

ECONOMIC IMPLICATIONS

13. Improving the environment in which legitimate users may use the computer and the Internet with greater security should facilitate even greater application of information technology in a wide spectrum of business, personal and other activities in Hong Kong, and should help enhance Hong Kong's competitiveness as an e-commerce hub.

PUBLIC CONSULTATION

14. Given the Working Group's internal nature, it has not conducted any formal public consultation. However, it has held informal discussions with various interested parties such as ISPs and academics. It has also briefed the Information Infrastructure Advisory Committee on its work and sought views from that committee. In addition, some of its members have visited the United States and exchanged views with relevant organizations there.

PUBLICITY

15. We will release the report for public consultation for two months from 1 December 2000. A press release will be issued, and briefings for the Legislative Council Panel on Security and the media will be arranged.

File Reference : SBCR 14/3231/88

Subject Officer : Mr. John LEE Ka-chiu, CAS/F (Tel. : 2810 2973)

Security Bureau
30 November 2000

[MIS1059.DOC]