立法會
Legislative Council

LC Paper No. CB(1)435/06-07(06)

Ref: CB1/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 11 December 2006

Background brief on information security

Purpose

This paper summarizes members' views and concerns on the issue of information security.

Background

2. In the wake of incidents involving leakage of personal data information on the Internet, the Panel discussed the subject of information security at the meeting held on 17 March 2006. At the subsequent meeting held on 6 April 2006, the Panel decided to follow up the subject, and requested the Administration to provide a comprehensive report of the current state of information security in policy bureaux and government departments (B/Ds) as well as publicly-funded bodies.

Information security framework of bureaux and departments

3. A set of information security policy, guidelines and procedures have been developed for use by B/Ds with reference to international best practice. These include a Baseline information technology (IT) Security Policy, IT Security Guidelines, Security Risk Assessment and Audit Guidelines, and Information Security Incident Handling Guidelines. These procedures and guidelines are reviewed from time to time to reflect changes in technology and security threats. They cover the organizational, management, technical and procedural aspects to enable B/Ds to build up their information security framework and practice. B/Ds are also required to comply with the Government's Security Regulations, which has a section covering information systems and related topics on the storage, processing and transmission of information, including classified information, cryptographic key management, physical security, and proper destruction of classified information.

4. To oversee and enforce information security within the Government, an Information Security Management Committee (ISMC) with core members from the Security Bureau and the Office of the Government Chief Information Officer (OGCIO) was established in 2000. An IT Security Working Group (ITSWG) has also been set up as an executive arm of the ISMC in the promulgation and compliance monitoring of IT security policies and guidelines among B/Ds.

5. At the central level, a Government Information Security Incident Response Office (GIRO) has been set up to co-ordinate and support all departments in the handling of Government information security incidents. To support the GIRO, a Standing Office in OGCIO monitors round the clock computer virus and information security incidents, outbreaks or alarms from all sources globally, and reports to the relevant units in the security framework as and when necessary. Virus alerts and security reminders are issued to departments as soon as a security problem is identified and assessed to be serious. Administrators of major government infrastructure systems will submit weekly information reports to the OGCIO on the security status of their systems and other issues relating to IT security for management monitoring and control purposes.

6. At the departmental level, all departments are required to appoint a senior officer to be the Departmental IT Security Officer who is responsible for the overall information security management and operation of the department. In addition, an Information Security Incident Response Team is set up in every department to deal with all matters on a day-to-day basis relating to security incident reporting and response. The IT Management Team in each department will work with the relevant Head of Department to keep watch on information security of the departments concerned.

Panel members' major views and concerns

7. While acknowledging that the Government has put in place a comprehensive set of information security policy and guidelines for use by B/Ds, members are concerned as to ***whether the established policies and guidelines are duly followed by B/Ds***. Moreover, members are also concerned about ***the information security status of publicly-funded bodies***, as well as ***how various regulatory bodies ensure their industry players' compliance with information security practices and requirements***.

LegCo question on information security

8. At the LegCo meeting held on 6 December 2006, Hon SIN Chung-kai raised a question on information security. In gist, the Hon Member expressed concern on the effectiveness of the measures adopted by ISMC and ITSWG in enhancing the information protection capabilities within the Government, and the overall information protection capabilities of public organizations. In reply, the

Administration has advised that in ensuring B/Ds' compliance with information security requirements, B/Ds are required to conduct information security risk assessment and review their information systems regularly. An annual information security survey is also conducted on B/Ds. These procedures and measures have proven to be effective in enhancing the overall security status of B/Ds. Concerning the information protection capabilities of public organizations, OGCIO conducted a survey in March 2006 through B/Ds on the information security protection measures implemented by major public organizations under their purview, and noted that the organizations have adopted various measures to protect themselves against information security threats. Another survey on the information security status of public organizations was conducted in August 2006, and the Administration will report the findings to the Panel at the meeting scheduled for 11 December 2006. (Hon SIN Chung-kai's question and the Administration's written reply are at **Appendix I**.)

Latest position

9. The Administration has been requested to brief members on the following at the meeting to be held on 11 December 2006:

(a) the current state of information security in B/Ds;

(b) how various regulators exercise their monitoring role to ensure that information security is being observed and complied with by the relevant sectors under their respective regulatory purviews; and

(c) measures taken by publicly-funded bodies to maintain and enhance information security (including those publicly-funded bodies which have declined to provide the requisite information for Panel's reference).

Relevant papers

10. A list of relevant papers is at **Appendix II**.

Council Business Division 1
Legislative Council Secretariat
8 December 2006

Appendix I

(Translation)

LEGCO QUESTION NO.17
(Written Reply)

Asked by: Hon SIN Chung-kai Date of Meeting: 6 December 2006

Replied by: Secretary for Commerce, Industry and Technology

Question:

In view of the recent cases in which the personal data of members of the public have been leaked by government departments and public bodies, will the Government inform this Council:

(a) of the measures currently adopted by the Information Security Management Committee and the Information Technology Security Working Group, so as to ensure that various policy bureaux and government departments comply with the information technology ("IT") security policies and guidelines formulated by the Government Chief Information Officer;

(b) whether it has assessed if the above measures can effectively enhance the information protection capabilities within the Government; if it has, of the assessment results; if not, the reasons for that;

(c) whether it has assessed the overall information protection capabilities of policy bureaux, government departments and public bodies; if it has, of the results; if not, whether it plans to make such assessment; if so, of the relevant details;

(d) whether it will consider extending the scope of application of the IT security guidelines to all public bodies to protect the personal data of members of the public; and

(e) whether it plans to allocate additional resources, including funding for information security projects and investment in hardware to improve the information protection capabilities of policy bureaux, government departments and public bodies?

Reply:

Madam President:

(a) The Information Security Management Committee (ISMC) and the IT Security Working Group were established to oversee information security within the Government. The ISMC has formulated and promulgated comprehensive IT security policies, procedures and guidelines that all bureaux and departments (B/Ds) are required to comply with. In ensuring their compliance with information security requirements, B/Ds are required to conduct information security risk assessment and review their information systems regularly. On the handling of information security incidents, the Government Information Security Incident Response Office (GIRO) provides central advice and co-ordination to B/Ds whereas individual B/Ds are required to appoint a senior officer to be the Departmental Information Security Officer (DITSO) to take charge of the overall information security management and operation of the department. In addition, each department has to set up an Information Security Incident Response Team (ISIRT) to deal with security incident reporting and response matters.

(b) The OGCIO works closely with relevant B/Ds on information security matters, and regularly reviews Government's related regulations, policies and guidelines to keep them in pace with the advancement of technology and the development of international and industry best practices. Besides, an annual information security survey is conducted on B/Ds, which has enabled us to keep in view of the implementation of IT security measures by the departments as well as provided necessary input for us to continuously enhance the information security management framework and technical measures being deployed. These procedures and measures have proven to be effective in enhancing the overall security status of B/Ds.

(c) An annual information security survey is conducted on B/Ds to enable us to keep in view of the implementation of IT security measures by the B/Ds and the recent one was completed in July 2006. In March 2006, the OGCIO also conducted a survey through B/Ds regarding the information security protection measures implemented by major public organisations under their purview. B/Ds have reported that the

organisations have adopted various measures to protect themselves against information security threats.

In August 2006, the OGCIO solicited the assistance of B/Ds to conduct another survey on the information security status of public organisations which B/Ds have purview over. A report on information security covering the overall security status of the B/Ds and public organisations has been produced and will be tabled at the LegCo IT & Broadcasting Panel Meeting to be held on 11 December 2006 for discussion.

(d) The OGCIO has advised B/Ds to encourage public organisations under their purview to adopt the information security guidelines where applicable. These guidelines are publicly available for access on the information security website (www.infosec.gov.hk). Moreover, we will cooperate with the Privacy Commissioner's Office and relevant industry bodies in promoting the importance of personal data privacy protection.

(e) B/Ds are responsible for implementing and enhancing their information security and may apply for funding for information security projects through the existing funding procedures. The capital expenditures for projects to review and enhance information security are chargeable to CWRF Head 710 Computerisation. Regarding the public organisations, they are responsible for their own investment, resources and funding on information security matters.

Appendix II

List of relevant papers

Committee	Paper	LC Paper No.
Meeting of Panel on Information Technology and Broadcasting (ITB) on 17 March 2006	✧ Administration's paper : "Information Security"	CB(1)1097/05-06(01)
	✧ Questions from Hon SIN Chung-kai on "Information Security"	CB(1)1096/05-06(07)
	✧ Administration's response to questions raised by Hon SIN Chung-kai on "Information Security"	CB(1)1214/05-06(01)
	✧ Minutes of meeting	CB(1)1382/05-06
Meeting of Panel on ITB on 6 April 2006	✧ Minutes of meeting	CB(1)1600/05-06