立法會
Legislative Council

LC Paper No. CB(1)2063/06-07(01)

Ref: CB1/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 9 July 2007

Updated background brief on information security

Purpose

This paper provides an update on the subject of information security and summarizes members' latest concerns on the issue.

Background

2. Information security has become a major issue of concern following the series of incidents involving leakage of personal data information on the Internet in early 2006. According to the Administration, the Government has a set of information security policy and guidelines for use by Government bureaux/departments (B/Ds). It has also put in place the management structure, technical security measures and other security mechanisms to monitor, detect and block suspected and potential attacks on the computer systems and networks within the Government. Details of these measures are set out in the "Background brief on information security" (LC Paper No. CB(1)435/06-07(06)) which can be browsed at http://www.legco.gov.hk/yr06-07/english/panels/itb/papers/itb1211cb1-435-6-e.pdf.

3. As regards the Government's role over publicly-funded bodies, the Administration advises that the Government monitors the information security status of public organizations and regulatory bodies through the responsible B/Ds which have purview over those organizations/bodies. Concerning the information security measures adopted by public organizations, generally speaking, such measures include security management framework, policy or guidelines on information security, security patch management, security risk assessment and audit, and incident and response management, etc. As for regulatory bodies, the information security measures adopted generally include mandatory information security management, risk assessment/audit/review, information security incident procedures, etc. (For details, please refer to the

Administration's paper (LC Paper No. CB(1)435/06-07(05)) which can be browsed at http://www.legco.gov.hk/yr06-07/english/panels/itb/papers/itb1211cb1-435-5-e.pdf.

4. In the wake of the incidents involving leakage of personal data information on the Internet, the Panel discussed the subject at the meeting held on 17 March 2006. At the subsequent meeting held on 6 April 2006, the Panel requested the Administration to provide a comprehensive report on the status of information security in B/Ds, as well as public organizations and regulatory bodies.

Report on the information security status of B/Ds, public organizations and regulatory bodies

5. In response to the Panel's request for a comprehensive report on the information security status of B/Ds, public organizations and regulatory bodies, the Administration conducted surveys on B/Ds, public organizations and regulatory bodies. The findings of the surveys were reported to the Panel at its meeting held on 11 December 2006.

6. Members have noted from the findings of the survey on B/Ds that there are comprehensive management framework and well-established policy and guidelines promulgated from the centre for compliance by B/Ds. About 84% of B/Ds had completed their information technology (IT) security risk assessment and audit, and the rest would complete the exercise before the end of March 2007. All B/Ds that had implemented mission critical systems had contingency measures in the form of business continuity plan and/or disaster recovery plan to handle cyber security incidents. Moreover, all B/Ds applied patch management to ensure that software vulnerabilities were properly fixed. Nevertheless, to enhance the effectiveness of security compliance of B/Ds, a new mechanism has been put in place by the Government to require all B/Ds to submit to the Office of the Government Chief Information Officer (OGCIO) annual reports on their compliance with government information security requirements, so that any irregularity can be identified at an early stage. Moreover, a centrally managed process in the form of security audits is also introduced to conduct random/sample checks on B/Ds in order to confirm that the necessary security risk assessments and reviews have been satisfactorily performed, and any recommendations for improvement are properly dealt with by B/Ds. The audit process has already been started in early 2007 and will cover all B/Ds over a period of two years.

7. In the case of public organizations and regulatory bodies, however, members have noted that as revealed by the survey, while 40% of the public organizations have not established an information security management framework and 41% do not have information security policies or guidelines, as many as 41% have not adopted any kind of security risk assessment and audit for information security assurance, and 34% of them even have no such plan for the

near future. On the prevention of restricted/classified data from unintentional disclosure, 43% do not utilize any technical tools such as cryptographic tools during their storage, transmission and processing of such data. Regarding regulatory bodies, 85% of them have not established mandatory information security management framework, 62% have not conducted risk assessment/audit/review, and 31% have not put in place information security incident procedures.

8. Details of the findings of the above two surveys can be browsed at http://www.legco.gov.hk/yr06-07/english/panels/itb/papers/itb1211cb1-435-5-e.pdf.

Members' concerns

9. In view of the aforesaid information security status of public organizations and regulatory bodies, and the Administration's remark that there is an urgent need for improvement in some public organizations and regulatory bodies, members have expressed grave concern on the information security status of public organizations and regulatory bodies, and considered that the responsible B/Ds should follow up with the public organizations/regulatory bodies under their purview measures to be taken on security protection improvements as soon as possible. The Administration should also make an interim report in a few months' time outlining the progress of public organizations/regulatory bodies in taking up follow-up actions, and brief the Panel on the subject again in July 2007. The Panel also considers that the Administration should disclose, for the Panel's reference, the names of those public organizations which have urgent need for improvement but still fail to improve their information security status when the Panel revisits the subject in July 2007.

Interim progress report on the information security improvements made by the public organizations and regulatory bodies

10. The Administration provided the captioned interim progress report in April 2007. According to the Administration, as of 12 March 2007, 96 out of 104 public organizations and 43 out of 58 regulatory bodies provided their progress updates on the improvements made to information security. Regarding the public organizations, while 28% of them have already completed their enhancement programmes, 29% have started their implementation works with a view to completing the required improvements by mid/end 2007. Yet, 43% reported that they could not implement all the improvement items within 2007 due to various reasons such as the need for policy endorsement, funding, projects alignment, or the sourcing of technical solutions and training courses. Nevertheless, the critical improvement items have been either completed or the work initiated.

11. With respect to regulatory bodies, 39% of them indicated that they already had regulatory regime emphasizing the importance of information security and protection of personal data, and 12% of them had action plans to enhance the information security of their regulated sectors. The remaining 49% considered that there was no provision for them to govern information security of the regulated sector under the present regulatory regime; nevertheless, nearly half of them will take actions to enhance the information security of their sector.

Latest position

12. The Administration will provide an updated progress report on the information security improvements made by public organizations and regulatory bodies at the Panel meeting to be held on 9 July 2007.

Relevant papers

13. A list of relevant papers is at the **Appendix**.

Council Business Division 1
Legislative Council Secretariat
5 July 2007

Appendix

List of relevant papers

Committee	Paper	LC Paper No.

Meeting of Panel on Information Technology and Broadcasting (ITB Panel) on 17 March 2006	✧ Administration's paper : "Information Security"
	✧ Questions from Hon SIN Chung-kai on "Information Security"
	✧ Administration's response to questions raised by Hon SIN Chung-kai on "Information Security"
	✧ Minutes of meeting
		CB(1)1097/05-06(01)
		CB(1)1096/05-06(07)
		CB(1)1214/05-06(01)
		CB(1)1382/05-06

Meeting of ITB Panel on 6 April 2006	✧ Minutes of meeting	CB(1)1600/05-06

Meeting of ITB Panel on 11 December 2006	✧ Administration's paper : "Information Security"
	✧ Background brief on information security
	✧ Follow-up paper : "Information Security"
	✧ Minutes of meeting
		CB(1)435/06-07(05)
		CB(1)435/06-07(06)
		CB(1)1329/06-07(01)
		CB(1)669/06-07