For Information
on 9 July 2007

Legislative Council Panel on Information Technology and Broadcasting

Information Security

A. Purpose

This paper updates Members on the progress of information security improvements made by the public organizations and regulatory bodies; and the security programmes being conducted for Government bureaux and departments (B/Ds).

B. Background

2. In July and August 2006, the Office of the Government Chief Information Officer (OGCIO) conducted surveys on the information security status of B/Ds, public organizations and regulated sectors. Based on the survey findings, the Information Technology and Broadcasting (ITB) Panel meeting of the Legislative Council (LegCo) held on 11 December 2006 advised that the identified improvements should be performed as soon as possible and requested the Administration to report on the work progress in July 2007 with an interim status updating report in 3 months.

C. Summary of Progress

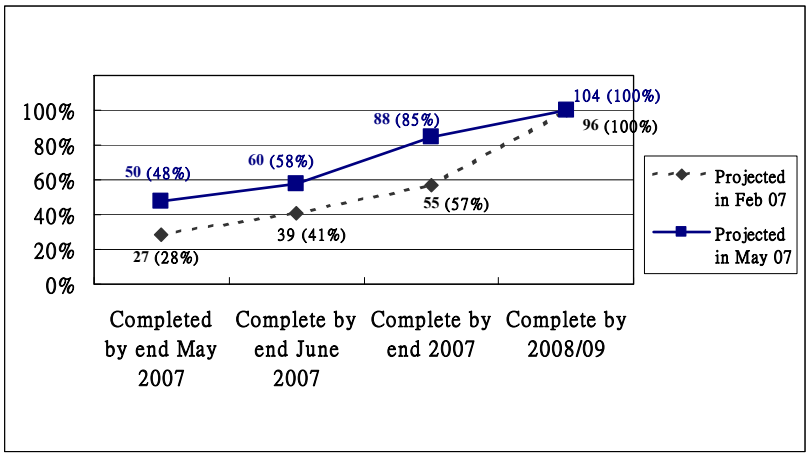
3. On 27 December 2006, the Government Chief Information Officer (GCIO) advised the responsible B/Ds to follow up on the security protection improvement and the exposures represented by the status quo of the public organizations and regulatory bodies under their purview pursuant to the findings from the survey. On 13 February 2007, the GCIO sought the B/Ds' coordination and support to collect the progress update on improvements made by these organizations. An interim status update report was compiled and submitted to ITB Panel in early April 2007.

4. On 21 May 2007, the GCIO sought the B/Ds' assistance again to coordinate and collect the progress updates on information security enhancement measures made by these organizations for compiling the required report for submission to the LegCo in July 2007. With their continuing support, all returns of the 104 public organizations and 58 regulated sectors surveyed were received by 13 June 2007.

D. Public Organizations

5. According to the data collected, further progress has been made by the public organizations in implementing their identified improvements. At end of May, 50 (48%) of the 104 public organizations have already completed all their enhancement work while 88 (85%) will finish by end of 2007. This compares favourably with the interim progress of 27 (28%) and 55 (57%) respectively as shown below.

Figure-1 – Progress of implementation by number of public organizations



6. Sixteen (15%) organizations reported that they could not finish their improvement work within 2007 although they had partially completed their enhancement programmes and 8 of them would finish within the 2007/08 fiscal year. Their main reasons for an extended implementation schedule were due to the interdependency of some tasks.

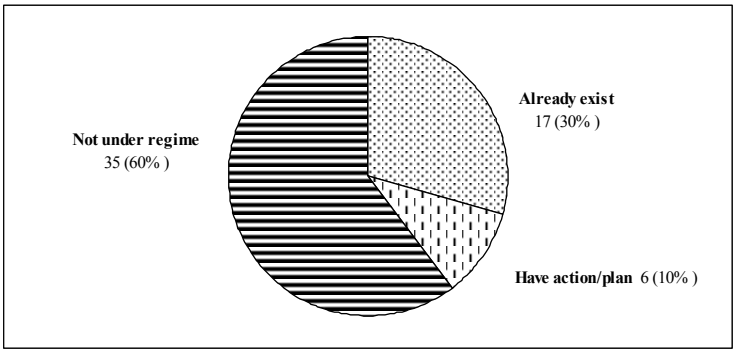
7. In terms of the number of improvement measures, 661 items (75%) were completed at end of May out of 884 identified in total while about 97% will be done within 2007. The remaining 3% of works are mainly to conduct security risk assessment and system audit, improve the contract provisions in IT outsourcing and implement more advanced security protection functions. A summary of the implementation progress grouped by six categories of security measures is provided in **Annex** for reference. They cover security management, security governance, adoption of security technologies, handling restricted/classified information, staff awareness and training, and IT services outsourcing.

8. According to the returns, there had been continuous progress in all six categories. In particular, a number of the public organizations had completed their improvement programmes on Staff Awareness and Training as advised by GCIO through the B/Ds having purview over them. Steady improvement is also shown in IT Services Outsourcing as many of the public organizations had strengthened their contractual provisions, quality assurance and security governance aspects to ensure contractor compliance with their information security requirements.

E. Regulated Sectors

9. All the 58 regulated sectors provided their returns. Our finding shows that the overall status of individual regulated sectors having or will put in place the necessary information security measures had only slightly changed by the report of one more sector. Thirty-five regulated sectors considered that there was no provision for them to govern information security of the regulated sector under the present regulatory regime.

Figure-2 – Status of tightening regulatory regime on the regulated sectors



10. In addition to tightening the regulatory regime, some regulatory bodies indicated that they would take actions to enhance the information security of their sectors such as issuing of reminders to their regulated sectors on the need for protection of personal data of their clients and employees; requesting their regulated sector to observe and comply with the practice circulars on information security in the course of their practice; urging their regulated sectors to make reference to the Government's information security policies and guidelines; and advising on good practices on information security during regular inspection visits.

F. Government B/Ds

11. Information security is the personal responsibility of every Government servant, who is subject to the general guidance by the Security Regulations on the handling of Government information. As far as electronic information is concerned, B/Ds are specifically required to comply with the requirements promulgated from time to time by OGCIO. In order to strengthen the monitoring of the compliance of B/Ds with the information security policy, the Government has launched a centrally managed process in the form of security audits. This will include checking the successful conduct of security risk assessments and reviews done by B/Ds and the recommended follow-up measures for improvements. Starting from May 2007, the security audits will examine all B/Ds over a 2-year period. Heads of B/Ds are responsible for security arrangements to protect all sorts of Government information in their own B/Ds, and to initiate action in cases of breach of security, including disciplinary actions in accordance with the relevant Government regulations.

12. To strengthen the overall information security governance in Government, and facilitate B/Ds in carrying out their management responsibilities on information security, B/Ds are requested to submit an annual report endorsed by their senior management to OGCIO, on their compliance with Government's information security regulations and policies in the form of a self-assessment checklist. The reports will provide input for the Government to formulate new work plan in further enhancing the overall information security posture.

13. To raise staff awareness in information security and data protection, Government has employed multiple channels to deliver training materials including E-learning courses and classroom seminars on various security topics. Specially designed for executive officers, a new series of seminars on "Government Information Security" has been started in May 2007 to enhance their knowledge and skills in their daily departmental operations.

G. Conclusion

14. The findings have indicated that the public organizations and regulatory bodies are increasingly aware of the importance of information security and data protection. The survey exercises have raised their management attention and staff awareness through implementation of the improvement measures to strengthen their security posture. As information security is an ongoing concern, the public organizations and regulatory bodies should stay vigilant of online threats and continue to enhance their security posture to protect their computer assets and restricted/classified data held by them. For Government, we are continuing to enhance our information security and data protection status through regular compliance checks, security audits and effective staff training programme.

H. Way Forward

15. To keep up the management attention, staff awareness and strengthening of security protection measures of the public organizations and regulated sectors, the Government will continue to monitor their information security enhancement programmes and provide advice and assistance through their responsible B/Ds. The OGCIO will regularly update the Government's one-stop information security portal (www.infosec.gov.hk) to provide the latest news, up-to-date reference information and security alerts to B/Ds and users in the public as well as collaborate actively with relevant industry players in promoting awareness and training on information security.

I. Advice Sought

16. Members are invited to note the contents of this paper.

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau
July 2007

Annex

Implementation Progress by Category of Security Measures

Category of Security Measures	Number of recommended measures				
	Completed by end February 2007	Completed by end May 2007	Planned to complete by end June 2007	Planned to complete by end 2007	Planned to complete within 2008/09
Security Management	98 (40.3%)	178 (73.3%)	188 (77.4%)	235 (96.7%)	243 (100%)
Security Governance	67 (42.1%)	112 (70.4%)	122 (76.7%)	156 (98.1%)	159 (100%)
Adoption of Security Technologies	63 (51.2%)	91 (74.0%)	94 (76.4%)	115 (93.5%)	123 (100%)
Handling of Restricted /Classified Information	43 (46.7%)	70 (76.1%)	75 (81.5%)	89 (96.7%)	92 (100%)
Staff Awareness and Training	52 (53.1%)	78 (79.6%)	82 (83.7%)	97 (99.0%)	98 (100%)
IT Services Outsourcing	95 (56.2%)	132 (78.1%)	141 (83.4%)	164 (97.0%)	169 (100%)
Total	**418 (47.3%)**	**661 (74.8%)**	**702 (79.4%)**	**856 (96.8%) (see Note below)**	**884 (100%)**

Note: The remaining 3.2% of identified improvement measures are mainly conduct of security risk assessment and system audit, improve the contract provisions in IT outsourcing and implement more advanced security protection functions.

Key aspects represented by the category of security measures:

Category	Key aspects
Security Management	Policy and Management, Operational Protection Measures, Contingency Handling, Security Risk Assessment and Audit
Security Governance	Test of Compliance, Supportive and Random Checks
Adoption of Security Technologies	Basic Tools, Special Data Handling Measures, Network Related, Asset Protection
Handling of Restricted /Classified Information	Operational Measures, Technical Tools
Staff Awareness and Training	Facilitation, Incentive for Staff to Acquire Information Security Qualification, Periodic Reminder
IT Services Outsourcing	Contractual Provisions, Qualify Assurance and Control, Security Governance and Control