LC Paper No. CB(1)1329/06-07(01)

For Information
April 2007

Legislative Council Panel on Information Technology and Broadcasting

Information Security

A. Purpose

This paper updates Members on the interim progress of information security improvements made by the public organizations and regulatory bodies.

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 Government bureaux and departments (B/Ds), public organizations and regulated sectors. Based on the survey findings, the Information Technology and Broadcasting (ITB) Panel meeting of the Legislative Council 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 March 2007.

C. Improvement Areas

3. On public organizations, six categories of information security enhancements involving a total of 884 work items were identified by the survey mentioned above-

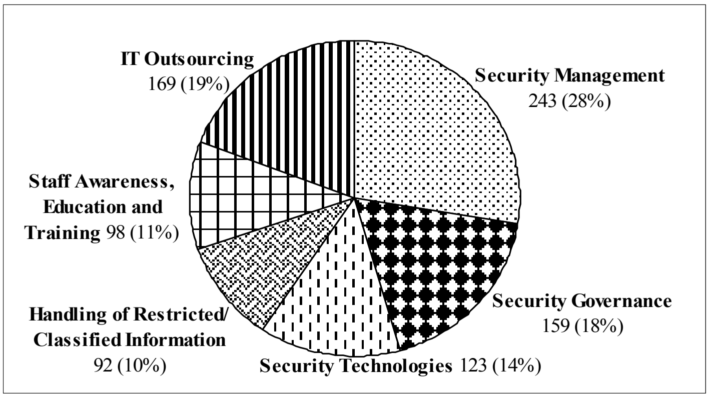


Figure 1 – Distribution of improvement items of public organizations

4. The survey also revealed that there is room for improvement in the regulated sectors on information security protection measures. The regulatory bodies were advised to consider tightening the regulatory regime to emphasize the importance of information security and protection of personal data in order to forestall incidents including data leakage.

5. On 27 December 2006, the Government Chief Information Officer (GCIO) wrote to individual Heads of B/Ds advising them on the specific improvement areas relevant to the public organizations and regulatory bodies under their purview, and B/Ds were also requested to coordinate the information security improvement programmes. They were also advised through their responsible B/Ds to make reference to the Government's information security policy and related guidelines in strengthening their information security status.

D. Progress To-Date

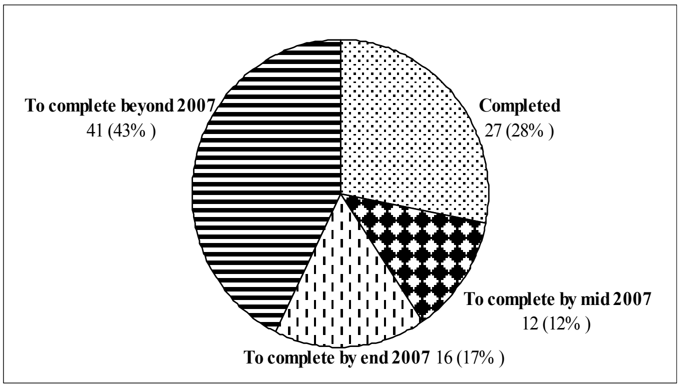
Response to Progress Updates

6. On 13 February 2007, the OGCIO requested B/Ds to coordinate and collect the progress updates on the improvements made by the public organizations and regulatory bodies under their purview. As of 12 March 2007, 96 out of 104 public organizations (92%) and 43 out of 58 regulated sectors (74%) have responded.

7. The OGCIO has subsequently issued reminders on 16 March 2007 and 23 March 2007 to the B/Ds that are responsible for the outstanding 8 public organizations and 15 regulated sectors. The B/Ds are liaising with these organizations to complete their returns at the time of this report.

Implementation by Public Organizations

Figure 2 – Implementation schedule of the improvement programmes by public organizations



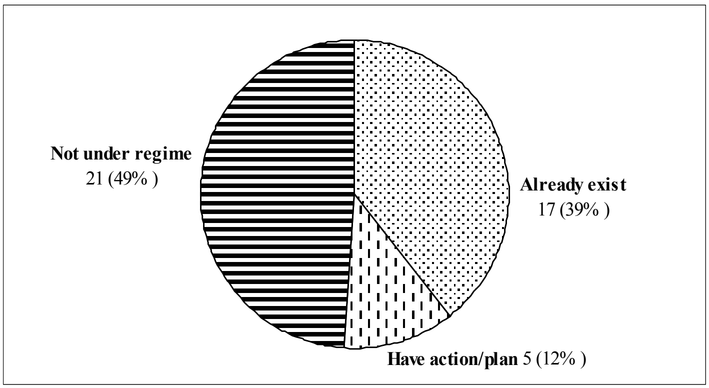
8. According to the returns received, 27 of the public organizations (28%) have already completed their enhancement programmes. The rest (69) have started their implementation works with 12 (12%) of them planning to complete the required improvements by mid 2007 and 16 (17%) by end 2007.

9. Forty-one (41) public organizations (43%) reported that they could not implement all the improvement items within 2007 due to various reasons concerning the need for policy endorsement, funding, projects alignment, or the sourcing of technical solutions and training courses. However, the critical improvement items have been either completed or the work initiated according to their reports.

10. A summary of the progress is provided in **Annex** for reference.

Implementation by Regulated Sectors

Figure 3 – Status of completion of improvements by regulated sectors



11. According to the 43 received returns, 17 of the regulated sectors (39%) indicated that they already had regulatory regime emphasizing the importance of information security and protection of personal data and 5 of them (12%) had action plans to enhance the information security of their regulated sectors.

12. The remaining 21 regulated sectors (49%) considered that there was no provision for them to govern information security of the regulated sector under the present regulatory regime but 9 of them would nonetheless take actions to enhance the information security of their sector.

E. Way Forward

13. The OGCIO will continue to urge the concerned B/Ds having purview over those public organizations and the regulatory bodies that have not responded to the request for progress updates. We will provide the necessary advice to the B/Ds in order to help them coordinate the improvement programmes. We will submit a work progress report to the ITB Panel in July 2007.

F. Advice Sought

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

Office of the Government Chief Information Officer
Commerce, Industry and Technology Bureau
April 2007

Annex

Summary of the Implementation Progress

Security Management

1. The progress of the 220 improvement items is shown below-

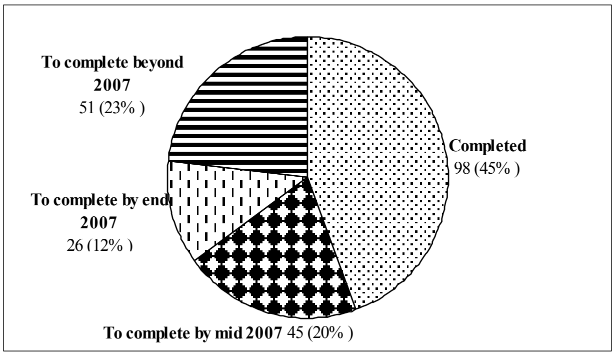


Figure 4 – Status of completion of 220 *Security Management* items[1]

2. The reasons given for the 51 items that could only be completed beyond 2007 include the need for seeking policy and financial support, the development of IT security policy and the establishment of management structure.

Security Governance

3. The progress of the 145 improvement items is shown below-

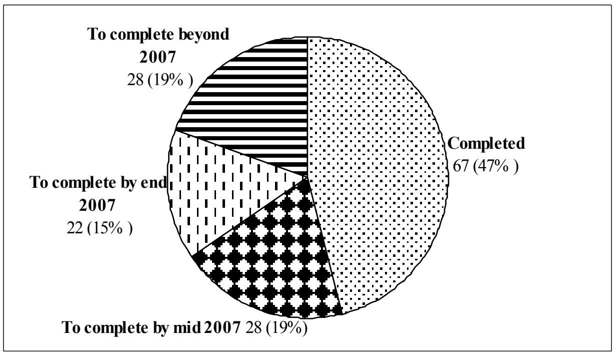


Figure 5 – Status of completion of 145 *Security Governance* items[2]

4. The reasons given for the 28 items that could only be completed beyond 2007 include the need to wait for the outcome of the security risk assessment and audit exercise to be completed in 2008.

[1] Examples of ***Security Management*** items include establishing proper management structure; defining information security policies and guidelines; enhancing operational protection measures; devising contingency planning measures; mandating staff awareness on information security; carrying out information security risk assessment and audit.

[2] Examples of ***Security Governance*** items include testing the compliance of security management measures by regular review and recovery drill; carrying out supportive and random checks.

Security Technologies

5. The progress of the 114 improvement items is shown below-

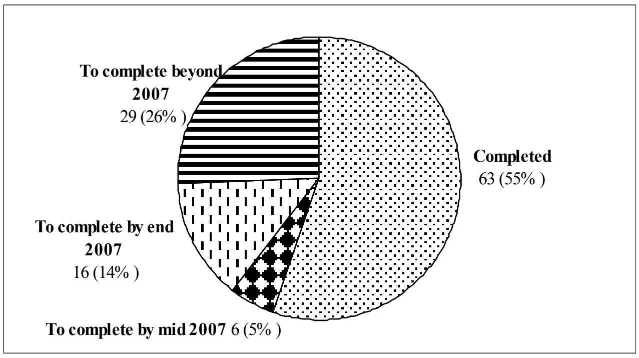


Figure 6 – Status of completion of 114 *Security Technologies* items[3]

6. The reasons given for the 29 items that could only be completed beyond 2007 include the need to source the suitable technical solutions such as patch management tools and anti-spyware tools.

Handling of Restricted/Classified Information

7. The progress of the 89 improvement items is shown below-

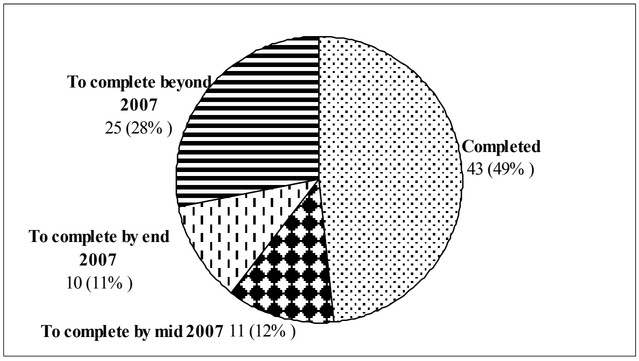


Figure 7 – Status of completion of 89 *Handling of Restricted / Classified Information* items[4]

8. The reasons given for the 25 items that could only be completed beyond 2007 include the need to source a suitable encryption tool.

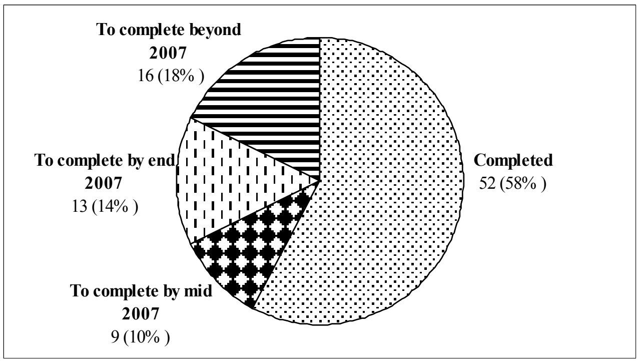
[3] Examples of ***Security Technologies*** items include adopting security patch application and management tools, anti-spyware tools, file/data encryption tools, secure data removal tools, intrusion detection/prevention tools; implementing backup and disaster recovery.

[4] Examples of ***Handling of Restricted/Classified Information*** items include enhancing operational measures by defining the classification of data, establishing procedures for granting of access to data, developing control procedures for staff access; encrypting the data.

Staff Awareness, Education and Training

9. The progress of the 90 improvement items is shown below-

Figure 8 – Status of completion of 90 *Staff Awareness, Education and Training* items[5]

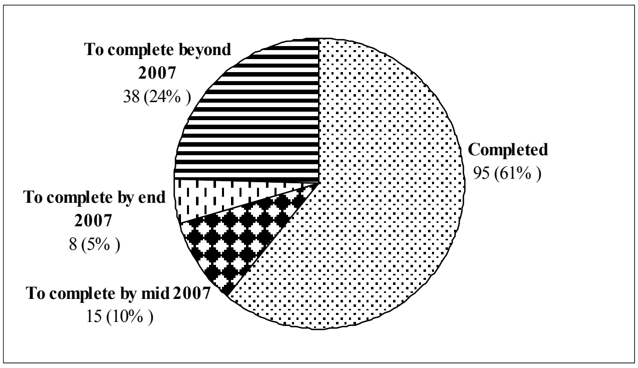


10. The reasons given for the 16 items that could only be completed beyond 2007 include the need to source the appropriate training courses in the market.

IT Outsourcing

11. The progress of the 156 improvement items is shown below-

Figure 9 – Status of completion of 156 *IT Outsourcing* items[6]



12. The reasons given for the 38 items that could only be completed beyond 2007 include the introduction of contractual provisions to tie in with the signing of new contracts or contract renewal.

[5] Examples of ***Staff Awareness, Education and Training*** items include organizing internal training and external training; providing incentives to encourage staff to acquire qualifications in information security skills; issuing periodic reminders.

[6] Examples of ***IT Outsourcing*** items include improving contractual provisions by clearly defining the roles and responsibilities of the contractor in data confidentiality, access control, change control, escalation process and incident response; tightening quality assurance and control in different testing stages; implementing regular compliance check.