立法會
Legislative Council

LC Paper No. CB(1)2465/09-10(05)

Ref. : CB1/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 12 July 2010

Updated background brief on information security

Purpose

This paper gives a summary of views and concerns raised by Members during previous discussions on information security in relation to the series of personal data leakage incidents involving Government bureaux/departments and public bodies.

Background

2. In early April 2008, some Police's internal documents were found on the Internet through the search engine of the peer-to-peer sharing software. On 22 April 2008, a Medical and Health Officer of the Tuen Mun Child Assessment Centre (TMCAC) reported loss of a portable USB drive, which contained working files and identifiable personal data of clients, at her office cum consultation room in TMCAC. On 23 April 2008, a portable electronic storage device containing information on two disciplinary inquiries conducted by the Civil Service Bureau was reported missing. The names and post titles of 25 serving civil servants were stored in such storage device. On 7 May 2008, the Immigration Department discovered that some confidential information of the department was found on the Internet through the search engine of a file sharing software. It was later identified that a new Immigration Officer had copied a number of sample documents from two senior officers to his home's personal computer causing leakage of information. In early May 2008, 10 incidents of loss of portable electronic devices which contained patient data of the Hospital Authority had been reported.

3. In the wake of the series of incidents of the loss of USB device containing personal data held by Government bureaux/departments and public hospitals, Members expressed grave concern about the protection of personal data, safeguarding information security and the handling of sensitive personal data by the Government and public bodies.

Previous discussions

4. At its special meeting on 30 May 2008, the Panel on Information Technology and Broadcasting (the ITB Panel) followed up the personal and sensitive data leakage incidents (involving the Civil Service Bureau, Hong Kong Police Force, Immigration Department, Department of Health and the Hospital Authority), the remedial measures undertaken by the Administration and the enhancement programmes to be pursued with a view to reducing the risk of further leakage. The Administration further updated the Panel on 8 December 2008 and 13 July 2009 on the progress of the follow-up actions taken and improvements made. Panel members' views and concerns raised at these meetings were summarized in the ensuing paragraphs.

Measures to prevent further data leakage by the Government and public bodies

5. In view of the concerns about the security risks on data protection involving the Government and public bodies, Panel members were keen to ensure that appropriate measures were in place to reduce the risk of further leakage and prevent recurrence of similar incidents to restore public confidence. Given the convenience and the popular use of the Internet and portable electronic storage devices, some members urged the Administration to adopt advanced data protection technologies, such as advanced USB flash drives with encryption and password lockdown, and virtual private network notebook computer using a secure network with encryption and authentication features. Some members suggested that Government bureaux/departments should check whether any classified Government documents were circulating on the Internet through the use of Foxy or other peer-to-peer file sharing applications, and take immediate action to remove such documents from the Internet. Members were also keen to ensure that international security standards were adopted across Government bureaux/departments, and that measures were in place to safeguard the Government IT system and websites from malicious attacks. They also urged the Administration to encourage private sector companies to strengthen their information security posture, and to increase the resources to the Hong Kong Computer Emergency Response Team Coordination Centre to enable it to better assist private business enterprises to enhance their information security capability.

6. Panel members expressed concern that the data leakage incidents involving Government bureaux/departments and public bodies revealed the prevalence of staff taking confidential documents and sensitive data home for work as this posed risk of data leakage. Some members were of the view that the management should also be responsible, to a certain extent, for the data leakage. If taking work home was necessary for operational reasons, the Administration/management should set out clear guidelines, put in place measures to ensure safe transit of data between home and office, and provide a secure computing environment for staff authorized to work at home. Members considered that Government should ascertain the extent of staff taking sensitive data to work at home and draw up quantifiable yardsticks as benchmarks to measure the level of staff awareness, so as to assess the effectiveness of the security enhancement measures. Staff should also be provided with technical

support and advice and education to raise their awareness of security issues. Enforcement and internal management should be strengthened to ensure compliance with the relevant security regulations and guidelines. Some members considered that disciplinary actions and a formal record in staff performance appraisal file would be effective deterrents for civil servants who had not exercised sufficient care and prudence in handling sensitive or personal data.

7. The Administration acknowledged the low level of staff awareness about information security, and the need to step up internal information security management and strengthen relevant security regulations. Continued effort would be made to promote staff awareness of security measures and guidelines through education and training, enhance technical and procedural measures, as well as strengthen management arrangements and enforcement to ensure compliance.

Notifying the Privacy Commissioner for Personal Data and affected data subjects of data leakage incidents

8. Some ITB Panel members expressed concern that the Privacy Commissioner for Personal Data (PCPD) had not been notified of all personal data leakage incidents involving Government bureaux/departments and public bodies, and the cases only came to light through media reports. Members urged the Administration to disclose all data leakage cases, and notify PCPD of all personal data leakage and the affected data subjects as far as practicable. Members also called on the bureaux/departments concerned to cooperate with PCPD upon PCPD's enquiry into the cases which had not been reported to PCPD.

9. The Administration advised that within the Government, all security incidents in electronic form would be reported to the Government Information Security Incident Response Office and PCPD would be notified of all incidents involving leakage of personal data in electronic form. The issue of whether it should be made a mandatory practice to report all losses of personal data in paper form to PCPD would be further examined. The affected data subjects, except those for whom there was no sufficient contact information for follow-up, would be notified of the leakage as far as practicable. Exception to these rules were permitted only when there was an overriding public interest consideration, in which case the approval of the head of the bureau/department concerned would have to be sought.

Power and functions of the Privacy Commissioner for Personal Data

10. The ITB Panel noted that all data users in the public and private sectors were subject to the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) governing privacy and personal data security, and were required to take every practicable steps to avoid unauthorized disclosure of all sensitive data, either in paper or electronic form. In this connection, members of the ITB Panel considered that PCPD should be provided with sufficient manpower and resources to discharge its statutory function of safeguarding and protecting personal data security. They also called for a review of

the PDPO as soon as practicable to ensure sufficient protection of personal data, and to make breaches of privacy a criminal offence.

11. The Administration advised that the review of PDPO would go through the necessary consultation and legislative procedures. The Consultation Document on Review of the PDPO was published on 28 August 2009 to invite public views on the proposals to amend the PDPO. As the Panel on Constitutional Affairs (CA Panel) was responsible for monitoring issues relating to personal data protection, the Administration would brief the CA Panel on the outcome of the consultation in due course.

Security of Wi-Fi facilities at Government venues

12. Dr Hon Samson TAM raised a question on security of Wi-Fi facilities at Government venues at the Council meeting on 26 May 2010. In response to the Member's concern about the encryption security of the wireless network access points at all Government premises and public education to further enhance public awareness of the security when using such facilities, the Administration advised that no non-compliance was found in the security risk assessment and annual audit of the Government Wi-Fi facilities in 2008 and 2009. Publicity and educational activities including Announcements in the Public Interest, roving shows, public seminars and publicity campaigns had been organized to educate the public about the importance of Wi-Fi security, remind users on setting up appropriate security detection and protection measures, and promote smart use of mobile Internet services.

Latest position

13. The Administration will brief the ITB Panel on the progress of Government's information security enhancement programmes. PCPD is also invited to update members on actions taken/being taken in the data leakage cases that have been reported to his Office through Government bureaux/departments since July 2009.

Relevant papers

Paper provided by the Administration for the Information Technology and Broadcasting Panel meeting on 30 May 2008
http://www.legco.gov.hk/yr07-08/english/panels/itb/papers/itb0530cb1-1679-1-e.pdf

Paper provided by the Hospital Authority for the Information Technology and Broadcasting Panel meeting on 30 May 2008
http://www.legco.gov.hk/yr07-08/english/panels/itb/papers/itb0530cb1-1679-2-e.pdf

Minutes of Information Technology and Broadcasting Panel meeting on 30 May 2008
http://www.legco.gov.hk/yr07-08/english/panels/itb/minutes/itb080530.pdf

Paper provided by the Administration for the Information Technology and Broadcasting Panel meeting on 8 December 2008
http://www.legco.gov.hk/yr08-09/english/panels/itb/papers/itb1208cb1-326-4-e.pdf

Background brief prepared by the Legislative Council Secretariat for the Information Technology and Broadcasting Panel meeting on 8 December 2008
http://www.legco.gov.hk/yr08-09/english/panels/itb/papers/itb1208cb1-326-5-e.pdf

Minutes of Information Technology and Broadcasting Panel meeting on 8 December 2008
http://www.legco.gov.hk/yr08-09/english/panels/itb/minutes/itb20081208.pdf

Paper provided by the Administration for the Information Technology and Broadcasting Panel meeting on 13 July 2009
http://www.legco.gov.hk/yr08-09/english/panels/itb/papers/itb0713cb1-2180-7-e.pdf

Paper provided by the Office of the Privacy Commissioner for Personal Data for the Information Technology and Broadcasting Panel meeting on 13 July 2009
http://www.legco.gov.hk/yr08-09/english/panels/itb/papers/itb0713cb1-2180-8-e.pdf

Background brief prepared by the Legislative Council Secretariat for the Information Technology and Broadcasting Panel meeting on 13 July 2009
http://www.legco.gov.hk/yr08-09/english/panels/itb/papers/itb0713cb1-2180-9-e.pdf

Minutes of Information Technology and Broadcasting Panel meeting on 13 July 2009
http://www.legco.gov.hk/yr08-09/english/panels/itb/minutes/itb20090713.pdf

Question No. 8 at the Council meeting on 26 May 2010 on "Security of Wi-Fi facilities in government venues"
http://www.info.gov.hk/gia/general/201005/26/P201005260160.htm

Council Business Division 1
Legislative Council Secretariat
8 July 2010