立法會
Legislative Council

LC Paper No. CB(1)2407/10-11(07)

Ref. : CB1/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 13 June 2011

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.

Information Security Enhancement Programmes in the Government

3. In the wake of the series of incidents of the leakage/misuse of 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.

4. The Administration subsequently rolled out the Information Security Enhancement Programmes in 2008, which aimed to better protect personal and sensitive data, and to ensure that bureaux/departments comply with the provisions of the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) by requiring them to take all practical steps to prevent unauthorized disclosure of personal data. The Programmes involved improving staff awareness and education, enriching technical and procedural measures, regularizing security risk assessments and monitoring, and reviewing security regulations, policies and guidelines.

Previous discussions

Panel on Information Technology and Broadcasting

5. Members have followed up the issue of information security since 2008. 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 (HKPF), 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, 13 July 2009 and 12 July 2010 on the progress of the follow-up actions taken and improvements made. Views and concerns raised at these Panel meetings were summarized in the ensuing paragraphs.

Enhancing information security posture

6. In view of the concerns about the security risks on data protection involving the Government and public bodies, members of the ITB Panel 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. Panel members urged that international security standards should be 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.

7. During the Panel meetings held in 2008 and 2009, 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. They considered that the management was responsible, to a certain extent, for such 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. These 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 other 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.

8. At the Panel meetings in 2008 and 2009, 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. The Administration undertook to make continued effort 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.

9. When the issue of information security was discussed at the ITB Panel meeting on 12 July 2010, members referred to the cases in the Privacy Commissioner for Personal Data (PCPD)'s report that some police files were found accessible on the Internet by Foxy users. Panel members noted that PCPD had concluded its investigation into these cases and was satisfied that HKPF had taken appropriate and effective measures, including compliance with the enhanced procedures, to prevent the recurrence of similar incidents.

10. At the meeting on 12 July 2010, Panel members also noted that the HKPF had taken a multi-pronged approach to enhancing end-point security controls, providing staff with encrypted USB thumb drives and official notebook computers with tightened security controls, and implementing a virtual workstation environment to cater for the mobile computing needs of officers in carrying out their duties. Training and education programmes were organized regularly to educate officers about information security and risks of data leakage. More frequent security audits and compliance checks on various information systems and computing equipment for shared use were also conducted.

Notifying the PCPD of data leakage incidents and powers and functions of PCPD

11. At the meeting on 12 July 2010, Panel members expressed concern that the PCPD had not been notified of all personal data leakage incidents involving Government bureaux/departments and public bodies, and that the cases came to light only through media reports. The Administration advised that following a review, it had been made a standing practice that bureaux and departments would report all cases involving personal data to the PCPD. 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. PCPD advised that his office had published a new Guidance Note entitled "Data Breach Handling and the Giving of Breach Notifications" to assist data users in handling data breaches and to mitigate the loss and damage that might be caused to the data subjects concerned.

12. The ITB Panel noted that all data users in the public and private sectors were subject to 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, Panel members considered that PCPD should be provided with sufficient manpower and resources to discharge its statutory function of safeguarding and protecting personal data security.

Review of the PDPO

13. At the meeting on 12 July 2010, members of the ITB Panel noted that a review of the PDPO was underway. They urged the Administration to give consideration to introducing legislation to make breaches of privacy a criminal offence, and for persons who suffered from abuses of their personal data to seek legal redress and compensation. The Administration advised that it had no plan in this regard but disciplinary proceedings would be instituted in accordance with the established disciplinary mechanism against any breaches and non-compliance by staff.

Council meetings

14. Hon Paul TSE raised a question on security of government sensitive information at the Council meeting on 5 January 2011. In relation to the disclosing of confidential files relating to defence and foreign affairs of various jurisdictions including Hong Kong by the WikiLeaks[1], he urged the Administration to formulate policies and measures to immediately raise the security level of communications and messages/information exchanged within the Hong Kong SAR Government and those exchanged between it and the Central Government as well as government organizations of various countries.

15. Hon Cheung Hok-ming raised a question on lost Octopus cards at the Council meeting on 23 February 2011. He was concerned about the number of lost Octopus cards containing personal data, and urged the Octopus to formulate a mechanism or proof for claiming lost cards.

Recent developments

16. At the special meeting of the Finance Committee on 22 March 2011, Mr CHEUNG Hok-ming asked about the repeated outbreaks of personal data leakage incidents in medical institutions and educational establishments. He urged the Administration to improve the present situation by allocating sufficient resources to support the PCPD for the effective enforcement of the PDPO. Mr Jeffrey LAM raised a question on how the PCPD would step up proactive enforcement of the PDPO in the light of the Report on Public Consultation on Review of the PDPO. Ms Emily LAU also raised a question on the possibility of leakage of personal data caused by the development of the Electronic Health Record and ways to prevent leakage.

[1] WikiLeaks describes itself as a not-for-profit media organization that provides a secure and anonymous way for sources to leak information to its journalists. It accepts restricted or censored material of political, ethical, diplomatic or historical significance.

17. At its meeting on 16 May 2011, the Panel on Constitutional Affairs (CA Panel) received a briefing by PCPD on the work of his Office, including the review of the PDPO. The CA Panel noted that the Government had announced in April 2011 that proposals of granting criminal investigation and prosecution power to PCPD, empowering PCPD to award compensation to aggrieved data subjects and requiring data user to pay monetary penalty for serious contravention of Data Protection Principles under the PDPO would not be implemented. PCPD was disappointed to note the Administration's decision which did not appear to be in accord with rising public expectation to strengthen the sanctioning powers of the PCPD and to deter privacy contraventions more vigorously.

Latest position

18. The Administration will brief the ITB Panel on the progress of Government's information security enhancement initiatives since the last update on 12 July 2010. 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 2010.

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

Paper provided by the Administration for the Information Technology and Broadcasting Panel meeting on 12 July 2010
http://www.legco.gov.hk/yr09-10/english/panels/itb/papers/itb0712cb1-2465-3-e.pdf

Background brief prepared by the Legislative Council Secretariat for the Information Technology and Broadcasting Panel meeting on 12 July 2010
http://www.legco.gov.hk/yr09-10/english/panels/itb/papers/itb0712cb1-2465-5-e.pdf

Minutes of Information Technology and Broadcasting Panel meeting on 12 July 2010
http://www.legco.gov.hk/yr09-10/english/panels/itb/minutes/itb20100712.pdf

Question No. 20 at the Council meeting on 5 January 2011 on "security of government sensitive information"
http://www.info.gov.hk/gia/general/201101/05/P201101050128.htm

Question No. 6 at the Council meeting on 23 February 2011 on "lost octopus cards"
http://www.info.gov.hk/gia/general/201102/23/P201102230114.htm

Questions raised at the special meeting of the Finance Committee on 22 March 2011
http://www.legco.gov.hk/yr10-11/english/fc/fc/w_q/cmab-e.pdf

Paper provided by the Office of the Privacy Commissioner for Personal Data for the Constitutional Affairs Panel meeting on 16 May 2011
http://www.legco.gov.hk/yr10-11/english/panels/ca/papers/ca0516cb2-1727-1-e.pdf

Background brief prepared by the Legislative Council Secretariat for the Constitutional Affairs Panel meeting on 16 May 2011
http://www.legco.gov.hk/yr10-11/english/panels/ca/papers/ca0516cb2-1741-3-e.pdf

Council Business Division 1
Legislative Council Secretariat
10 June 2011