立法會
Legislative Council

LC Paper No. CB(1)326/08-09(05)

Ref. : CB1/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 8 December 2008

Background brief on
information security in relation to the series of personal data leakage incidents involving Government bureaux/departments and public bodies

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 the wake of a series of incidents of the loss of USB memory sticks 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

General

3. Members followed closely the data leakage incidents and related issues at Council meetings and panel meetings. Questions pertaining to the data leakage incidents, the protection of privacy, the remedial/improvement measures undertaken by the Administration to safeguard information security, strengthen the protection of personal data and reduce the risk of further leakage, the handling of personal data by the Government/public bodies and business corporations, as well as the review of the Personal Data (Privacy) Ordinance (PDPO) (Cap. 486) were

raised at Council meetings on 21 May, 28 May and 11 June 2008. The Panel on Information Technology and Broadcasting (ITB Panel) and the Panel on Home Affairs had also discussed the relevant issues in the previous legislative term.

4. In general, Members were gravely concerned about the widespread leakage of sensitive personal data and urged for improvement measures to further enhance information security, safeguard privacy and forestall further leakage. They called for a tightening of information security regulations and policies to uphold a high standard of information security among the Government and public bodies to prevent the recurrence of similar incidents. Members were keen to ensure that an effective monitoring mechanism was in place to strengthen the protection of privacy and ensure compliance by staff handling personal data, thereby enhancing the public's confidence in the handling of personal data by the Government, public bodies and business corporations.

5. At its special meeting on 30 May 2008, the ITB Panel received a briefing by the Administration (including the Office of the Government Chief Information Officer, Civil Service Bureau, HKPF, ImmD, DH) and representatives of HA and the Privacy Commissioner for Personal Data (PCPD) on the background to the incidents, remedial measures undertaken by the Administration and the enhancement programmes to be pursued with a view to reducing the risk of further leakage. Members' views and concerns raised at the meeting were summarized in the ensuing paragraphs.

Notifying affected data subjects/HKPF/PCPD of data leakage incidents

6. Noting that HKPF, PCPD and some of the affected data subjects were not notified of the leakage incidents, some members expressed concern about the selective notification to the concerned parties and the lack of a standard practice among Government bureaux/departments to alert the affected data subjects or report the incidents to the HKPF and/or PCPD. Members also enquired whether the Government/public bodies involved in the leakage incidents would commit themselves to be responsible for any loss suffered by the affected data subjects arising from the incidents, as in the case of the Hong Kong and Shanghai Banking Corporation. At members' request, the Administration had provided a summary of personal data leakage incidents over the past three years (**Appendix I**) for the Panel's information. According to the summary, affected citizens in 24 out of the 30 incidents had been notified of the leakage. For those cases where affected citizens were not notified, it was mainly because of insufficient contact information. The issue of whether notifying affected data subjects and PCPD of the leakage incidents should be made mandatory would be addressed in the coming review of information security policies and the PDPO. As regards compensation to persons affected by the leakage, members noted that presently there were no statutory provisions or resources for PCPD's office to assist data subjects in claiming damages. Data subjects whose personal data were compromised could seek damages through civil proceedings.

Disciplinary action against staff causing data leakage

7. Members were concerned how cases of abuse of personal data had been dealt with and whether disciplinary actions had been taken against those staff for non-compliance with security regulations. The Administration advised that the Government bureaux/departments involved in the date leakage incidents had either completed or were making thorough investigations into the leakage. Disciplinary proceedings would be instituted in accordance with the established disciplinary mechanism against any breaches and non-compliance. Penalties ranging from advice to dismissal would be imposed as appropriate depending on the nature and seriousness of the breaches. The Administration would update the Panel on findings of the investigations.

Measures to prevent further data leakage

8. Members were keen to ensure that appropriate measures were in place to reduce the risk of further leakage and prevent recurrence of similar incidents so as to restore public confidence in the handling of personal data by the Government. Given the convenience and the popular use of the Internet and portable electronic storage devices as well as the need for staff to take home work for operational reasons, 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), to ensure that staff authorized to work at home was provided with a secure computing environment. Suggestion was also made for Government bureaux/departments to monitor the Internet, the Foxy and other peer-to-peer file sharing applications to search for any classified Government documents circulating on the Internet, so that immediate action could be taken to remove such documents.

Powers and functions of Privacy Commissioner of Personal Data

9. Members were concerned that the Office of the PCPD, being a statutory body funded by the Government to safeguard personal data security and protection, seemed to be a "toothless tiger" without power. As presently there were no statutory requirements for data users to report leakages of personal data to PCPD, the PCPD could only come to know about leakage through media enquiries and press reports. Members noted that the PCPD had earlier recommended to the Constitutional and Mainland Affairs Bureau amendments to the PDPO to expand PCPD's power in the coming PDPO review. The Administration would also consider whether the practice of reporting data leakage incidents to PCPD should be made mandatory.

Staff taking work home

10. Members raised concern about the prevalence of staff taking confidential documents and sensitive data home for work as this posed risk of data leakage.

Members urged the Administration to assess the extent of and reasons for staff taking work home. Some members were of the view that the management, to a certain extent, should also be responsible 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. It was suggested that the management should check and monitor the use of classified documents and alert their staff to the potential danger of peer-to-peer file sharing applications and security risks. Enforcement and internal management should be strengthened to ensure compliance with the relevant security regulations and guidelines. Staff should also be provided with technical support and advice and education to raise their awareness of security issues.

11. Some members held the view that the leakage incidents were partly caused by the lack of resources, such as insufficient number of computers for use in the office, and heavy workloads. In this regard, the HKPF was urged to acquire more computers with word processing function for input of classified information. Members noted that the HKPF had set up a working group to conduct an overall review of IT security to examine the reasons for taking work home, the sufficiency of office computers as well as the use of personal computers for work at home. The Administration would brief the Panel on the findings of the working group.

Latest development

12. The Administration will update the Panel at the meeting on 8 December 2008, on progress of the follow-up actions taken and improvements made, and also the outcome of any investigations and review completed.

Reference

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

Council Business Division 1
Legislative Council Secretariat
4 December 2008

Appendix I

Government Bureaux / Departments (Summary of incidents involving leakage of personal data for last 3 years up to 22 May 2008)

B/D involved	Summary of the incident	Affected citizens	Informed affected citizens (Yes/No)	Informed Privacy Commissioner (Yes/No)	Informed Police (Yes/No)	Reason for not inform related parties
Civil Service Bureau	Civil Service Bureau reported that a portable electronic storage device containing information on two disciplinary inquiries was reported missing on 23 April 2008. The names and post titles of 25 serving civil servants were stored in the storage device.	25 (Civil servants)	Yes	Yes	Yes	Not applicable.
Department of Health	A Medical and Health Officer of the Tuen Mun Child Assessment Centre (TMCAC) reported loss of a portable USB drive at her office cum consultation room in TMCAC. The USB device contained working files and identifiable personal data of clients.	668	Yes	Yes	Yes	Not applicable
Education Bureau	A local press reported a data leakage incidence in November 2006 that an alumni list of about 200 teachers with information including the teacher's name, school name, school telephone	About 200	Yes	Yes	No	Information theft was not involved and no intrusion to information systems.

B/D involved	Summary of the incident	Affected citizens	Informed affected citizens (Yes/No)	Informed Privacy Commissioner (Yes/No)	Informed Police (Yes/No)	Reason for not inform related parties
	number and e-mail address was found on the EDB website. The list was uploaded with written consent of the concerned alumni to facilitate communication and professional interflow among themselves and did not carry serious implication. The information was removed immediately.					
Food and Environmental Hygiene Department						No criminal offence was involved for all cases and the affected citizens of two cases accepted the explanation and apologies from the department.
Case 1	The case is related to a food-related complaint. The incident occurred in April 2007. When issuing an enquiry letter to a member of the public, the officer inadvertently attached to it other personal data.	1	Yes	Yes	No	
Case 2	The case occurred in August 2007 and was also related to a food-related complaint. The officer used some	1	Yes	No	No	

B/D involved	Summary of the incident	Affected citizens	Informed affected citizens (Yes/No)	Informed Privacy Commissioner (Yes/No)	Informed Police (Yes/No)	Reason for not inform related parties
Case 3	used paper for printing a letter which was sent to a member of the public. It was later noticed that the overleaf of the letter contained the name and address of a third party. The incident happened in October 2006. In sending two letters to two prosecution witnesses in connection with a littering offence, a staff mixed up the envelopes. One of them thus noted the name and address of the other person; while the latter noted the similar information and means for communication of the former.	2	Yes	No	No	
Immigration Department	The Immigration Department was informed by the media on 7 May 2008 that some confidential information of the department could be found through the search engine of a file sharing software on the Internet. After investigation, it was identified that a new Immigration Officer has copied a	14	No	Yes	No	Due to insufficient contact information or restriction on use of the information, the affected citizens were not informed.

B/D involved	Summary of the incident	Affected citizens	Informed affected citizens (Yes/No)	Informed Privacy Commissioner (Yes/No)	Informed Police (Yes/No)	Reason for not inform related parties
	number of sample documents from two senior officers to his home's PC in order to familiarize the daily operations. It was suspected that this caused the leakage of information.					
Intellectual Property Department	In a report on 1 April 2007, a local newspaper reported that some personal data, including a photocopy of a passport, was uploaded through the IPD's system to the Internet where the public can read it.	180	Yes	Yes	No	Not applicable.
Leisure and Cultural Services Department	On 6 May 2006, LCSD was informed that the personal data about some guardians of participants of the 2009 East Asian Games Slogan Competition were found on the Google search engine.	4	Yes	Yes	Yes	Not applicable.
Police Force Case 1	In December 2006, the Police became aware that someone had uploaded non-sensitive personal data (including staff number, post title and office telephone number) of several	About 700	Yes	Yes	N/A	

B/D involved	Summary of the incident	Affected citizens	Informed affected citizens (Yes/No)	Informed Privacy Commissioner (Yes/No)	Informed Police (Yes/No)	Reason for not inform related parties
Case 2	hundreds of police officers and more than 20 old crime alert messages onto the Internet. In early April 2008, the Police became aware that some Police's internal documents could be found on the Internet through the search engine of the peer-to-peer sharing software. The Technology Crime Division in the Commercial Crime Bureau started investigation immediately.	About 20	Yes	Yes	N/A	
Post Office	The case involves a public complaint that 25 notification cards for the collection of Registered and Recorded Delivery items, which were torn apart but had not been destroyed by irreversible means (e.g. via a paper shredder), were found in a rubbish bin outside the rear entrance of On Ting Post Office in Tuen Mun.	25	No	Yes	No	The case was not crime related and there was insufficient information to contact affected users.
Social Welfare Department	In a staff's personal blog, names of 29 Comprehensive Social Security	29	No	Yes	Yes	PCO and Police were informed of the incident. The personal blog

B/D involved	Summary of the incident	Affected citizens	Informed affected citizens (Yes/No)	Informed Privacy Commissioner (Yes/No)	Informed Police (Yes/No)	Reason for not inform related parties
	Assistance recipients appeared in 26 episodes. In some of these episodes, information like their age and educational background was mentioned.					was deleted shortly after the case was reported to the Police.
Treasury	In January 2007, 15 e-Payslips were suspected to have been mis-directed to un-intended recipients. Subsequently, only 4 were confirmed to have been mis-directed. Matter has since been rectified.	15 (Civil servants)	Partly informed	No	Yes	Computer fraud was not involved. The Hong Kong Identity Card and bank account numbers on the payslips were partially masked.
Total	**14 cases**	**About 1,884**				

Public Organisations (Summary of incidents involving leakage of personal data for last 3 years up to 22 May 2008)

Organisation involved	Summary of the incident	Affected citizens	Informed affected citizens (Yes/No)	Informed Privacy Commissioner (Yes/No)	Informed Police (Yes/No)	Reason for not inform related parties
City University	A staff member of the University transferring inadvertently the personal data to a public server. The data involved the name, sex, HKID no, address, employment background, and education and professional background of applicants for admission of BEng(Hons) Building Engineering (Modern Structural Engineering) in 2005.	68	No	Yes	No	No criminal offence was involved.
Hospital Authority (10 cases)	Since 1 April 2007, HA has received 10 reports of loss of electronic devices which contain or might contain patient data. These cases concern six hospitals/clinics. Of these 10 cases, eight were reported to have taken place within hospital/clinic and two outside hospital/clinic premises. The electronic devices lost included five USB memory sticks, one palm handheld device, one MP3 player, one Central Processing	15 878	Yes Yes	No (8 Cases) Yes (2 Cases)	Yes Yes	PCO is following-up the cases. Not applicable.

Organisation involved	Summary of the incident	Affected citizens	Informed affected citizens (Yes/No)	Informed Privacy Commissioner (Yes/No)	Informed Police (Yes/No)	Reason for not inform related parties
	Unit, one laptop computer and one digital camera. Seven of the ten cases are suspected to be theft-related while lost of devices were involved in the remaining three cases.					
Hong Kong Institute of Education	On 5 March 2007, when announcing the 2007 Non-JUPAS offer list, application data of 204 non-JUPAS applicants of year 2006 was inadvertently included and uploaded to the Internet.	204	Yes	No (PCO approached the institute actively)	No	No criminal offence was involved. The information was removed about 30 minutes after announcement.
Hong Kong University Case 1	On 10 October 2007, a staff member of the University unintentionally pressed the wrong key and printed the content of a CD given by his friend through the University Computer Centre's network printer. The printed documents were believed to have contained the personal data of a number of non-HKU persons.	Insufficient information (The University did not own the information)	No	Yes	Yes	The University did not own the information. The Police was investigating the case.
Case 2	On 13 March 2006, a data file containing the personal data of some of	68	No	Yes	No	The leaked information was deleted immediately.

Organisation involved	Summary of the incident	Affected citizens	Informed affected citizens (Yes/No)	Informed Privacy Commissioner (Yes/No)	Informed Police (Yes/No)	Reason for not inform related parties
	the University's students was found to be accessible by the public through the Internet. The file was uploaded by a student to his personal web directory for printing purpose but forgot to remove it after printing.					
Independent Police Complaints Council	As reported by the media on 10 March 2006, the personal information about 20,000 people who complained against the police to the Independent Police Complaints Council (IPCC) were found on the Internet.	26 341	Yes	Yes	Yes	Not applicable.
Polytechnic University	The oversight of a technical staff to suspend a regular computer job before the scheduled time for sending the examination result notification to students led to system irregularities. As a result, some 1,780 students wrongly received emails containing other students' results.	1 780	Yes	Yes	No	Only information within the University was involved in the incident.
Total	**16 cases**	**44 339**				

Appendix II

List of relevant papers

Committee	Paper	LC Paper No.
Meeting of ITB Panel on 30 May 2008	Administration's paper on "Information Security" http://www.legco.gov.hk/yr07-08/english/panels/itb/papers/itb0530cb1-1679-1-e.pdf	CB(1)1679/07-08(01)
	Paper provided by the Hospital Authority http://www.legco.gov.hk/yr07-08/english/panels/itb/papers/itb0530cb1-1679-2-e.pdf	CB(1)1679/07-08(02)
	Minutes of meeting http://www.legco.gov.hk/yr07-08/english/panels/itb/minutes/itb080530.pdf	CB(1)2312/07-08
Meeting of Home Affairs Panel on 4 July 2008	Administration's paper on "Review of the Personal Data (Privacy) Ordinance" http://www.legco.gov.hk/yr07-08/english/panels/ha/papers/ha0704cb2-2488-1-e.pdf	CB(2)2488/07-08(01)
	Administration's paper on "Protection of personal data privacy" http://www.legco.gov.hk/yr07-08/english/panels/ha/papers/ha0704cb2-2454-1-e.pdf	CB(2)2454/07-08(01)
	Minutes of meeting http://www.legco.gov.hk/yr07-08/english/panels/ha/minutes/ha080704.pdf	CB(2)2850/07-08
Council meeting on 21 May 2008	Oral question no.4 raised by Hon Audrey EU Yuet-mee on "Protection of personal data" and the Administration's reply http://www.legco.gov.hk/yr07-08/english/panels/itb/papers/itb0530cb1-1679-3-c.pdf	CB(1)1679/07-08(03)
	Written question no. 15 raised by Hon Emily LAU on "Review of the Personal Data (Privacy) Ordinance" and the Administration's reply http://www.legco.gov.hk/yr07-08/english/panels/itb/papers/itb0530cb1-1679-4-e.pdf	CB(1)1679/07-08(04)
	Written question no. 19 raised by Hon CHEUNG Hok-ming on "Loss of patient	CB(1)1679/07-08(05)

Committee	Paper	LC Paper No.
	data stored in electronic devices" and the Administration's reply http://www.legco.gov.hk/yr07-08/english/panels/itb/papers/itb0530cb1-1679-5-e.pdf	
Council meeting on 28 May 2008	Oral question no. 1 raised by Hon Jasper TSANG Yok-sing on "Protection of personal data by government departments and public organizations" and the Administration's reply http://www.legco.gov.hk/yr07-08/english/panels/itb/papers/itb0530cb1-1692-1-e.pdf Written question no. 20 raised by Hon Emily LAU on "Loss of computer server containing personal data of customers by a bank" and the Administration's reply	CB(1)1692/07-08(01) Hansard
Council meeting on 11 June 2008	Oral question no. 3 raised by Hon Ronny TONG on "Government departments' handling of incidents of leakage of personal data " and the Administration's reply	Hansard