LC Paper No. CB(1)2465/09-10(03)

For Information
on 12 July 2010

Legislative Council Panel on Information Technology and Broadcasting

Information Security

Purpose

This paper informs Members about the progress of Government's information security enhancement programmes since the last update on 13 July 2009.

Background

2. The Government has continued to enhance the security measures in bureaux/departments (B/Ds) and provide support to the community for improving their information security status. The various security initiatives and updates are grouped under three main areas –

(a) information security enhancement programmes in the government;
(b) security posture in the government; and
(c) information security in the community.

Information Security Enhancement Programmes in the Government

3. In managing information security, prevention is a major success factor. The Information Security Enhancement Programmes aimed at improving staff awareness and education; enriching technical and procedural measures; regularising security risk assessments and monitoring; and reviewing security regulations, policies and guidelines.

(i) Staff Awareness and Education

4. In April 2009, the Office of the Government Chief Information Officer (OGCIO) launched a one-year staff communication programme on information security through a variety of communication methods and channels[1]. The programme has received positive support and feedback from staff. One of the activities conducted was a series of roving exhibitions at government offices in which over 12,000 staff participated. We have centrally organised training events regularly, as well as assisted B/Ds in customising courses to satisfy their specific needs, for example, a briefing on information security to newly recruited Executive Officers as a mandatory part of their induction programme.

5. We conducted staff surveys before and after the staff communication programme to assess its effectiveness. Based on the survey results, there is indication that the knowledge and attitude of staff towards information security have noticeably improved. For example, we found that the percentage of respondents that had read the IT security policy document at least once has been nearly doubled after the programme. We also found that the percentage of respondents who had a better understanding of the various kinds of emerging IT security threats has more than doubled.

6. In view of the growing use of social networks in the community and in some aspects of official duties in the Government, we have issued specific guidelines on the information security threats and aversion measures. We have reminded staff of the need for secure handling and disposal of data and sensitive information that may be stored in electronic devices of modern office equipment during day to day use, including photocopiers, facsimile machines and printers.

(ii) Technical and Procedural Measures

7. The OGCIO has continued to carry out surveillance on risks associated with IT development trends and identify security solutions

[1] These included developing and disseminating leaflets, posters and smart reminders; organising seminars and web training courses; producing video training materials, flash animations, articles and newsletter; as well as arranging roving exhibitions targeted at all levels of staff in the Government.

available in the market. This information is then provided to B/Ds for them to implement in protecting their systems and data. The Government Information Security Incident Response Office (GIRO) Standing Office also regularly issues security and virus alerts to remind and facilitate B/Ds to take timely actions to apply patches to fix software vulnerabilities, and follow security best practices in managing and operating their systems and databases.

8. In order to meet their operational security needs, some B/Ds, with the support of OGCIO, have also successfully developed and implemented security solutions on their information systems to further enhance remote access and strengthen end-user device and connectivity[2]. For example, the Hong Kong Police Force (HKPF) has taken a multi-pronged approach to enhancing end-point security controls, providing 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. HKPF also provides training and regularly broadcasts messages to educate officers about information security and risks of data leakage. It is performing more frequent security audits on various information systems, user compliance and computing equipment for shared use.

(iii) ***Strengthening the management arrangements to ensure compliance and to provide advice and support to B/Ds and public bodies***

Security Risk Assessments and Monitoring

9. According to the prevailing IT Security Policy, B/Ds are required to conduct regular departmental security risk assessment and audit. The OGCIO has reviewed and revised the process of conducting departmental security risk assessments and promulgated enhanced guidelines to B/Ds.

10. At the end of 2009, we streamlined the compliance monitoring and auditing processes co-ordinated through OGCIO. The refined monitoring mechanism includes drawing attention to more specific areas

[2] These included the employment of various technical measures such as virtual private network solutions to provide secure remote access, end-point protection solutions to enable access control policies, and virtualisation technology to establish a secured computing environment.

of concern, collecting inputs through surveys, conducting sample audits, and consolidating risk findings from B/Ds' departmental security risk assessments. By doing these, we should have a better understanding and closer monitoring of the security status and compliance of B/Ds, and B/Ds can detect and resolve security issues in a more proactive manner. This new mechanism will start operation in the 4th quarter of 2010.

Public Bodies

11. B/Ds and the relevant public bodies under their purview continue to exchange information on information security matters and coordinate on the implementation of appropriate protection measures against information security exposures. In May 2010, the OGCIO issued a reminder to B/Ds requesting them to draw the attention of public organisations under their purview to common and prevailing security threats which include phishing, malicious code attacks and loss of portable storage devices. Through the reminder, we have provided tips and techniques for protecting their information systems against these threats.

12. The Hospital Authority has continued to implement necessary measures to enhance security protection and mitigate against data exposure risks. **Annex 1** provides a summary of their progress.

(iv) Review of Information Security Regulations, Policies and Guidelines

13. Last year, OGCIO also completed a review of the information security aspects of the Government Security Regulations and promulgated the updated requirements to all B/Ds for them to follow. One of the changes is to make compulsory the notification procedures that have been adopted since the end of 2008. If personal data is involved in a security incident, B/Ds should report the case to the Office of the Privacy Commissioner for Personal Data (PCPD) as soon as possible and notify the affected individuals as far as practicable. To keep the regulations, policies and guidelines in pace with technology advancement, international developments, industry best practices and emerging security threats, we have also included emerging security topics such as endpoint access

control, and updated best practices such as encryption of Wi-Fi traffic using the latest encryption standard.

Security Posture in the Government

14. Although we cannot stop the occurrence of security incidents completely, the frequency of occurrences has shown signs of decreasing. In the first two quarters of 2010, the GIRO received four security incident reports all involving data leakage[3].

15. For the past 12 months since the last meeting of this Panel in July 2009, there have been eight cases of data leakage reported to the GIRO. These cases are summarised in **Annex 2**. One of these cases did not involve sensitive data. In two other cases involving loss of storage media, the data on the lost media have either been encrypted or were protected by access control mechanism. For all cases involving personal data, B/Ds have reported them to the PCPD and notified the affected individuals as appropriate.

Information Security in the Community at Large

Community Wide Activities

16. To enlist support from Internet Service Providers (ISPs) on cyber security, the OGCIO regularly teams up with HKPF and the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) to hold ISP Symposiums on various contemporary topics to keep the service providers abreast of the emerging threats that may impact on their operations; as well as to share and discuss how service providers, HKCERT and law enforcement agencies can collaborate to counter the attacks, for the betterment of the economy. To test the coordination amongst major stakeholders of Hong Kong’s Internet infrastructure during major incidents, an information security incident response drill will be conducted in October 2010.

[3] In the whole of 2009, there were 14 security incident reports of which 10 were related to data leakage.

17. The “Hong Kong Clean PC Day” campaign in 2009 was held successfully. The finale of the campaign was a public conference with the theme “Security of Online Transaction”. More than 90% of the respondents gave a very good rating during the review survey. As part of the “Hong Kong Clean PC Day” campaign in 2010, we have already held two free-of-charge public seminars in March and May. Another one will be held in November with a tentative theme on “Safe Online Social Networking”.

18. We have produced short episodes on tips and best practices on information security for broadcasting on the radio channel. In recent months, we have developed episodes around the theme of safety on social networking. We have also published articles on our information security portal (www.infosec.gov.hk) to help computer users understand the safety aspects of using online social networking services and remind youngsters to be aware of threats such as online grooming and cyber-bullying. In September 2009, the Government also launched a one-year Internet education campaign to promote the safe and healthy use of the Internet among students, parents and teachers.

Emerging Security Threats

19. Malicious codes, worms and botnets[4] are security threats being faced worldwide. The Government, collaborating with various parties, continues with our effort on enhancing information security awareness in the community so that businesses as well as citizens can realise the importance of protecting their computer assets. Since late 2008, a notorious computer worm[5] has infected a large number of computers in various countries. OGCIO has been working with the Hong Kong Internet Registration Corporation (HKIRC), HKCERT, and HKPF to monitor the development of the worm and detect any signs of activity that may affect Hong Kong. Through the collaboration, we have provided advice to potentially affected users as and when necessary.

20. We are aware that malicious codes on popular mobile platforms are emerging. With the widespread use of mobile communication devices

[4] A botnet is a network of computers that have been compromised without their owners' knowledge. These computers may be remotely controlled to perform malicious activities over the Internet.

[5] This computer worm is known as Conficker.

by citizens, the impact of malicious code infection becomes more notable with a multiplying effect. We are closely monitoring the information on computer security made available by international and local organisations to keep up-to-date with the trends of computer security attacks and solutions available against such attacks. We will share relevant information with the public through our one-stop information security portal.

Conclusion and Next Steps

21. In the past year, the Government continued to implement various enhancement programmes and activities to uphold our security posture. Due to emerging security threats, new business initiatives, use of new technologies and changing service models on the Internet, there are always new and evolving security risks. The task of maintaining a high standard security posture will continue to be challenging and we must keep ourselves vigilant in protecting the Government's data assets.

22. We have noticed higher demands in basic security training courses and will arrange more of such courses in the coming year. We will be strengthening our security governance to B/Ds under the new monitoring mechanism. Through the conduct of public awareness and education activities, we will continue to better equip citizens' ability in protecting themselves against cyber security threats. Information security in its entirety is not a one-off project. It is an iterative process that is as much about processes and people as it is about technology. We shall continue to update Members on this subject on an annual basis.

Advice Sought

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

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau
July 2010

Annex 1

ITB Panel Meeting on 12 July 2010

Progress of Actions taken by the Hospital Authority

Purpose

This note briefs Members on the status of actions taken by the Hospital Authority (HA) on enhancing the patient data security and privacy since the privacy incidents in 2008.

Background

2. The HA Task Force and PCPD have made 26 and 37 recommendations respectively on eight areas to further enhance the effectiveness of patient data protection covering the HA's policy, structure and people, staff awareness and training programme, procedures and guidelines, privacy impact assessment and containment, audit, contracts and technology. Action plan was developed and implemented to address the issues and recommendations.

Action Plan and Progress

3. The HA Board endorsed the action plan with 19 consolidated targets in September 2008 for addressing the recommendations from Task Force and PCPD in enhancing and strengthening the protection of patient data security and privacy.

4. The following summarizes actions that have been taken:

(a) To effectively oversee the Information Security and Privacy enhancement programme in the HA Head Office and in Clusters, governance structures were formed respectively, namely the HA Information Security and Privacy Committee, and Clusters Information Security and Privacy Committees. They are established in overseeing the implementation of action targets for HA wide in strengthening HA information security and privacy.

(b) Apart from the enhancement on the governance of Information Security and Privacy, HA and PCPD also jointly delivered the privacy awareness campaign for all hospitals. The objective was to raise the privacy awareness of HA staff in protecting the patient data privacy. Seminars were conducted during the period from May 2009 to March 2010.

(c) An e-Learning courseware was developed in 2009 as a standard education module for all staff in HA. It aimed at providing the essential knowledge on personal data protection as stipulated in the Personal Data (Privacy) Ordinance, and HA Information Security and Privacy policies. Staff of HA are requested to complete the courseware by end 2010.

(d) Procedures and Guidelines relating to Information Security and Privacy were reviewed and updated for staff in protecting patient data privacy in the workplace. Ongoing efforts are required and planned in promulgating them in an effective manner.

(e) Auditing on user access to the patient data was conducted in 1Q 2010 after the implementation of the access audit system. The audit will be periodically conducted to detect potential access violations.

(f) Technology improvements were implemented to protect the data during download and the data in the risky workstations against data leakages. Further strengthening are being planned for additional protection of the workstations.

5. A few action targets are progressively implemented with target dates extended due to software problems encountered prior to the implementation. The central file servers, secure email, and enforced encryption on end-point mobile devices are scheduled to complete in 2010/11.

Hospital Authority
June 2010

Annex 2

Summary of data leakage incidents in Government from July 2009 to June 2010

No.	Incident Date	Bureau/ Department	Summary of the Incident and follow-up measures
1	August 2009	Census and Statistics Department (C&SD)	A removable hard disk containing classified information was lost. The data involved was not sensitive as it is available from the Business Registration Office of Inland Revenue Department upon request of the public. No personal data was involved. The concerned officer was advised to observe the security guidelines when handling classified data.
2	October 2009	Labour and Welfare Bureau (LWB)	A USB drive which contained personal particulars of 2,666 participants of a consultancy study conducted by Polytechnic University (PolyU) was lost. LWB considered that the concerned data was not leaked as the USB drive was shortly recovered in the campus. All affected individuals were informed and the case was reported to the PCPD. Enhancement measures on data transfer and storage were implemented thereafter. The concerned staff of PolyU resigned after the incident.
3	December 2009	University Grants Committee (UGC) Secretariat	A web application had a fault in one of its preview functions which disclosed personal information of application users to a limited small group of other unintended users. The programming error was made by the IT contractor of UGC Secretariat. The case was reported to the PCPD and apologies were sent to six affected individuals. The programming error of the web application was identified and fixed. Disciplinary action was not applicable in this case.
4	December 2009	Hong Kong Police Force (HKPF)	Over 100 documents of HKPF dated from 2002 to 2008 were searchable through Foxy. The information included personal data of 118 staff and 83 citizens. HKPF had informed affected individuals and reported to the PCPD. Disciplinary reviews against concerned officers

No.	Incident Date	Bureau/ Department	Summary of the Incident and follow-up measures
			were either completed or in progress.
5	February 2010	Department of Health (DH)	A privately-owned USB drive which contained personal particulars including name and ID number of three individuals was lost. All affected individuals were informed and the case was verbally reported to the PCPD. Verbal warning was issued to the concerned staff.
6	April 2010	Leisure and Cultural Services Department (LCSD)	In a burglary case, one office computer containing personal data of 410 individuals (staff and their family members) was stolen. The stolen computer was protected with username and password, and further access control was applied to the concerned files containing personal data. The case was reported to the PCPD and all affected individuals were informed about the incident. Disciplinary action was not applicable in this case.
7	April 2010	Education Bureau (EDB)	An unauthorised access to a personal computer within a locked office was suspected. All files stored in one of the disk drive were deleted. Some of the deleted files containing personal data for about 20 individuals. The case was reported to the Police and PCPD. Notification to affected individuals and any needs of disciplinary action would be subject to result of investigation by the Police.
8	June 2010	Innovation and Technology Commission (ITC)	A member of the Panel of Assessors for the Innovation and Technology Support Programme (ITSP) under the Innovation and Technology Fund lost a compact disc (CD) containing information on project proposals seeking funding from ITSP and personal data of nine project members. The lost CD was password protected and all data was encrypted. The case was reported to the PCPD and all affected individuals were informed about the incident. The Panel member has also reported the loss to the Police. Disciplinary action was not applicable in this case.