For Information
on 13 July 2009

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 in December 2008.

Background

2. At the meeting of the Panel on Information Technology and Broadcasting (ITB Panel) on 8 December 2008, we briefed Members on the progress of Government's information security enhancement programmes. The aim of these programmes is to better protect personal and sensitive data and to ensure that bureaux/departments (B/Ds) comply with the provisions of the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) requiring them to take all practical steps to prevent unauthorised disclosure of personal data. The Government was requested to update the ITB Panel again on the progress of existing and planned security enhancement initiatives after six months.

3. Government accords great importance to the protection of personal and sensitive data. The enhancement initiatives comprise remedial actions to tackle problems as well as a series of coordinated activities undertaken by the Administration to safeguard information security, strengthen the protection of personal data and reduce the risk of further leakage.

Progress of Information Security Enhancement Programmes

4. The enhancement programmes cover four main areas: staff awareness and education, technical and procedural measures, security compliance checking and the review of security regulations, policies and guidelines. The following paragraphs describe the progress of the activities in each area.

(i) Staff Awareness and Education

5. Awareness and education are key factors to influence the behaviours of staff at the workplace. The Government aims to build and sustain a high level of staff awareness in order to enhance the overall information security status of Government B/Ds.

6. We conducted a staff survey at the beginning of the enhancement programmes in early 2009 to determine the current situation of staff awareness level regarding their attitude, knowledge of the subject and compliance with information security requirements. The findings are provided in **Annex 1**. In summary, most staff are concerned about incidents involving data protection matters and are receptive to activities promoting or strengthening information security.

7. On information security awareness, about 98% of the staff responding to the survey have rated data protection as important or very important suggesting that they are conscious of the need to handle data cautiously or securely. On knowledge of Government's security requirements, about 90% and 77% of them respectively have read the relevant parts of the government Security Regulations and the IT Security Policy. On their operational practices, respondents are following the best practices guidelines to protect their PCs and data. About 80% of them have implemented measures to protect their computers by passwords and habitually check that no classified document is left on printers when they are unattended.

8. The survey also revealed that staff who have read the security requirements are also behaving appropriately when handling personal

data.

Staff Communication Programme

9. A strong culture of security takes time to build up. Since early 2009, the Office of the Government Chief Information Officer (OGCIO) has rolled out a one year Staff Communication Programme (the Staff Programme) to address the findings from the staff survey and help Government staff build up and sustain a high level of awareness, working knowledge, good practices and a commitment to safeguarding classified and personal data. The Staff Programme aims to make staff respect and understand their responsibilities for the data entrusted to them.

10. We have employed a variety of communication tools and channels to ensure effective reach to different target groups, including leaflets and posters, smart reminders, customised seminars, web training courses, video training materials, newsletter articles, thematic web pages, games and quizzes, roving exhibitions and e-card design contest.

11. In April 2009, over 250 management and senior level staff from various B/Ds attended an information security conference organised by the OGCIO to share experience on office culture and practices to stop data leakage during the management, operation and delivery of government services. At the conference, senior officers from the OGCIO, Security Bureau and Civil Service Bureau (CSB) have emphasized to the audience and requested them to champion the security policy and initiatives in their B/Ds including according high priority to the adoption of suitable security mechanisms and helping staff acquire the knowledge and understanding of the appropriate data security measures.

Staff Training

12. We are committed to providing ongoing staff training to update colleagues and reinforcing their understanding of and care for information security. In the past 12 months, the centre has arranged over 20 classroom training sessions and seminars to more than 3,000 staff of various B/Ds. Details are provided in **Annex 2**. Some of these include train-the-trainers

courses. A training kit has been developed to facilitate B/Ds to tailor their own training materials so that B/Ds can conduct customised training to their staff, which can better align with their departmental objectives, business processes and operating environments.

13. The OGCIO and the Civil Service Training and Development Institute of CSB have jointly developed flexible training and learning arrangements for staff to take web-based training courses at their own pace. Since April this year, more than 2,600 staff have enrolled on various courses. In addition, we have arranged a standing contract for engagement of external service providers to provide training services to promote Government staff's awareness on data protection. Further rounds of training and seminars on Privacy and Data Protection have been planned for the rest of this year.

(ii) ***Technical and Procedural Measures***

Protection against data leakage through Peer-to-Peer software and Use of Portable Storage Devices

14. In February 2009, a circular on "Data Protection Against Risks of Using Peer-to-Peer (P2P) Software" was issued to all B/Ds to provide clear guidelines on the protection against possible data leakage, particularly when working outside the office or using privately-owned computers installed with P2P software. Besides reminding staff not to store or process classified information in privately-owned computing facilities including portable storage devices, they are also advised to regularly check and clean up their computers and storage devices (such as USB flash drives, CDs, floppy diskettes, etc.) of any official use personal or classified data that might have been left there unintentionally. All these steps are aimed at minimising the risk of leakage of data.

Technical Tools and Solutions

15. B/Ds are deploying various kinds of technical tools to protect data and encryption tools and solutions are the most widely deployed, which can minimise the risks of data exposure in the event of security

threats, hacking or loss of the storage media. Some B/Ds are also planning to adopt more sophisticated security solutions to assist in the control of the connection of USB devices to PCs.

16. The use of suitable technical tools and solutions will help staff prevent data leakage. We continue to provide B/Ds with the latest technology updates and technical solutions as well as technical seminars on data protection, such as encryption tools, end-point security solutions, and secure deletion tools.

(iii) ***Security Compliance Checking***

17. An independent security audit of all B/Ds managed by the OGCIO was completed in May 2009. The overall finding shows that B/Ds' information systems are in general compliant with Government's security requirements. Any identified weaknesses are being followed up properly and improvement measures put in place. The management of B/Ds have raised their attention and effort on data protection and staff training in order to enhance the awareness, knowledge and ability to comply with the security regulations and policies. In the B/Ds, unauthorised software especially P2P file sharing software is strictly prohibited on government-supplied computers while applicable security technologies including storage encryption, digital certificate and virtual private network have been deployed. Most B/Ds have demonstrated their capability to conduct their own departmental security risk assessments to a high standard. We will conduct periodic security audits in future.

18. As requested in the Panel meeting on 8 December 2008, an update of the security risk assessment of the Hong Kong Police Force (HKPF) is provided in **Annex 3**. Based on the outcome and findings of the independent security audit, the HKPF is complying with the security requirements insofar as the domain areas audited, although some improvements have been recommended by the auditor and are being pursued by HKPF. OGCIO will continue to follow up with HKPF.

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

19. The Government has established security regulations and policies including the requirement to comply with the provisions of the PDPO. It has been emphasized that if personal data is involved in a security incident, the responsible B/D should report the case to the Office of the Privacy Commissioner for Personal Data (PCPD) as soon as possible and notify affected individuals as far as practicable.

20. The Government regularly reviews the IT security related regulations, policies and guidelines to ensure that they are up-to-date with technological advancement, international developments and industry best practices. In January 2009, the OGCIO initiated a review and aims to promulgate the revised regulations, policies and guidelines by the end of 2009. The review will benchmark our security policies against those countries advanced in IT as well as international standards such as ISO27001, ISO27002 (published by International Organisation for Standardisation) and COBIT (Control Objectives for Information and related Technology). We will add practical user references for easy reading and understanding of the security requirements and effective day-to-day practice.

Government's information security posture

21. In 2008, 19 security incidents were reported[1] to the Government Information Security Incident Response Office (GIRO), which provides central co-ordination to B/Ds in the handling of Government information security incidents. In the first two quarters in 2009, ten incidents have been reported of which 6 were data leakage incidents. The other 4 cases were related to malicious attacks of Government websites (e.g. intrusion attempt) and fake websites. All these cases had been quickly remedied and no internal systems were affected. A summary of the data leakage incidents is provided in **Annex 4**. Although there were still data leakage cases in early 2009, the impact has been significantly

[1] Security incidents that need to be reported include: unauthorised access, denial of resources, disruption of services, leaks of classified data in electronic form, malicious destruction or modification of data / information, penetration and intrusion, computer viruses and hoaxes, and malicious codes or scripts affecting networked systems.

reduced due to the protection measures that are in place, e.g. the data or the lost storage devices had been protected by encryption. B/Ds have reported the relevant cases to the PCPD and notified the affected individuals as appropriate. B/Ds have taken appropriate actions against the concerned officers according to established procedure including necessary disciplinary action on those who have violated the security regulations and procedures.

Information Security in the Community at Large

Students and Teachers

22. Government continues to promote information security to the public with a focus on the proper use of computing facilities and ways to protect their computer resources and information assets. We have conducted 35 school visits with over 9,000 participants since the start of the school visit programme in early 2008. The visit programme was well-received by the participants and helped to convey important messages about online access safety to the target groups. In view of the good response and results, we will continue our visits to schools to deliver appreciation courses as well as providing advice on information security and the ethical use of IT and the Internet to students, teachers and parents.

23. Separately, Government is launching a one-year territory-wide Internet education campaign to teach Internet users especially young students on the proper and safe use of the Internet. This campaign will emphasise to young students the importance of and respect for personal data privacy and intellectual property rights, avoidance of internet addiction, protection against computer virus attacks, etc.

Business Enterprises

24. In recent years, Botnets[2] have increasingly threatened the health

[2] 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.

and safety of the Internet. In April 2009, the Conficker computer worm[3] caused a major security threat to users by infecting victim computers and turning them into members of a large, global Botnet. In collaboration with the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), we have closely monitored the Conficker worm and promptly advised computer users of the development and protection against its attack. Furthermore, in May 2009, the OGCIO, HKPF and HKCERT held an Internet Service Provider (ISP) Symposium to coordinate ISPs' effort against Botnets and enhance the security status of Hong Kong as a leading digital city. In the symposium, we briefed ISPs on the threats of Botnets and other security attacks that are related to their operation, and discussed how ISPs, HKCERT and law enforcement agencies can work together to crack down the attacks for the betterment of the economy.

25. Government is very supportive of security promotion events organised by private institutes or security associations for the public. During the past 12 months, senior officers of the OGCIO had given presentations in six major local security conferences delivering messages and advice on information security to the public.

26. We will carry out the fifth "Hong Kong Clean PC Day" campaign in 2009. This year we will focus on information security when conducting electronic transactions. The campaign is an annual programme to raise public awareness on information security and strengthen the protection of their computers from cyber attacks. A series of seminars will also be held in August and November specifically targeting public bodies and SMEs.

Public Bodies

27. We have regularly advised B/Ds to share the relevant policy, guidelines and technical information on information security with public bodies to enhance their security posture. In the recent security reminder issued in March 2009 to all B/Ds regarding the protection against the

[3] Conficker is a computer worm first appeared in October 2008. Since then, it has kept evolving and is believed to have infected millions of computers globally.

Conficker worm, we have again reminded them to inform public organisations and regulatory bodies under their purview. The OGCIO will continue to liaise closely with and help B/Ds in their provision of advice and assistance on information security matters to public organisations.

28. The Hospital Authority has continued to implement necessary measures to enhance security protection and mitigate against data exposure risks. **Annex 5** provides a summary of their progress.

Conclusion and next steps

29. Like all other enterprises, Government is not immune from information security risks including data leakage. Organisations worldwide have seen an epidemic growth in security breaches leaving few unscathed. We will uphold our information security policies and practices and will take steps to further enhance the level of trust that citizens have inherently given us in maintaining their personal and sensitive data.

30. There is no single panacea that will solve all security problems overnight or once and for all. We will continue to adopt a multi-pronged approach with a series of initiatives and activities to address the different information security needs in the Government and refreshing our programme as and when necessary. Our immediate target is to create a strong culture of security so that every staff will be an active participant in the prevention of data breaches. Such a culture needs time to develop and become entrenched. To keep Members apprised of the development, we propose to update the ITB Panel on the progress of the security initiatives in a year's time.

Advice Sought

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

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau
July 2009

Annex 1

ITB Panel Meeting on 13 July 2009

Initial Staff Awareness Survey in January 2009

Given the intangible nature of security awareness, a direct measurement of such qualities is difficult. This initial staff survey conducted in early 2009 assessed some of the factors related to staff awareness and education. Responses have been analysed to help show the situation on staff awareness level (what they think), staff knowledge (what they know) and their behaviour/commitment (what they do).

2. On the awareness level, the survey results showed that most civil servants are now quite conscious about data protection matters. **Figure 1** shows that about 98% of them rated data protection as important (22%) or very important (76%) suggesting that they are conscious of the need to handle data cautiously or securely. Staff's strong perceived importance of information security will make them more aware of securely handling of data and is the first step towards creating a security culture and this needs to be sustained by the promotion activities through various channels.

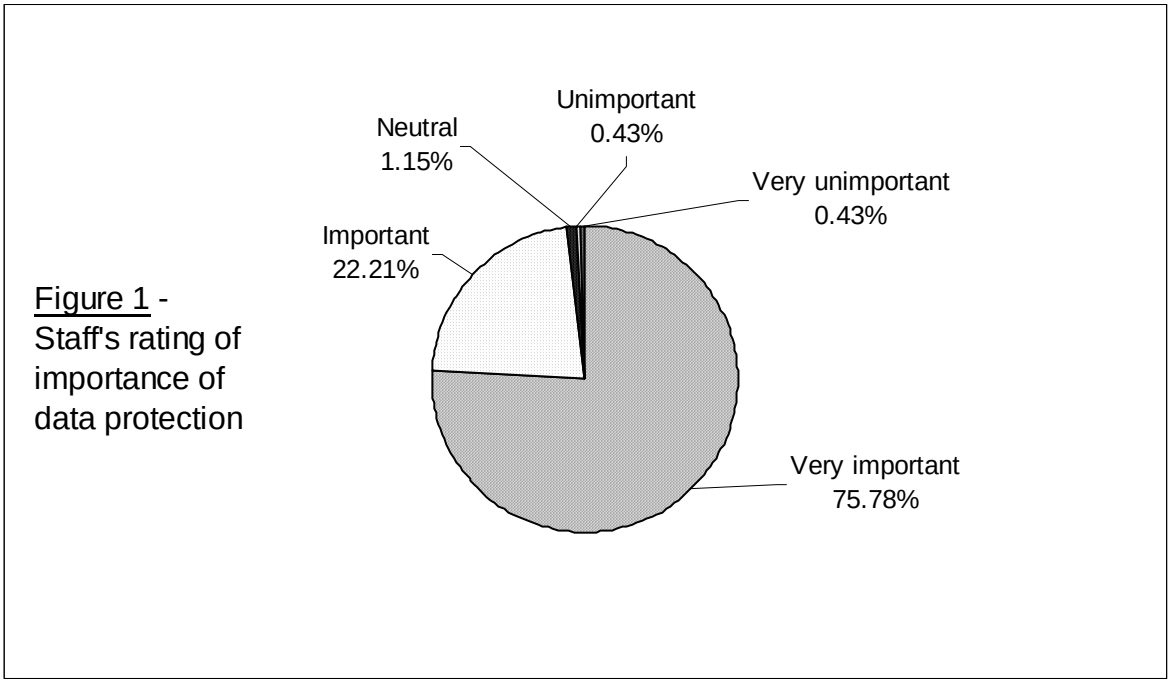


Figure 1 - Staff's rating of importance of data protection

3. On knowledge level, the findings showed that staff could improve their acquaintance with Government's Security Regulations and IT Security Policy. **Figure 2 and 3** show that about 90% of surveyed staff have read the Security Regulations (with some only on selected parts), while 77% have read the IT Security Policy (with some only on selected parts). The survey also revealed that in general those staff having better knowledge of the regulations have demonstrated better behaviours in data protection.

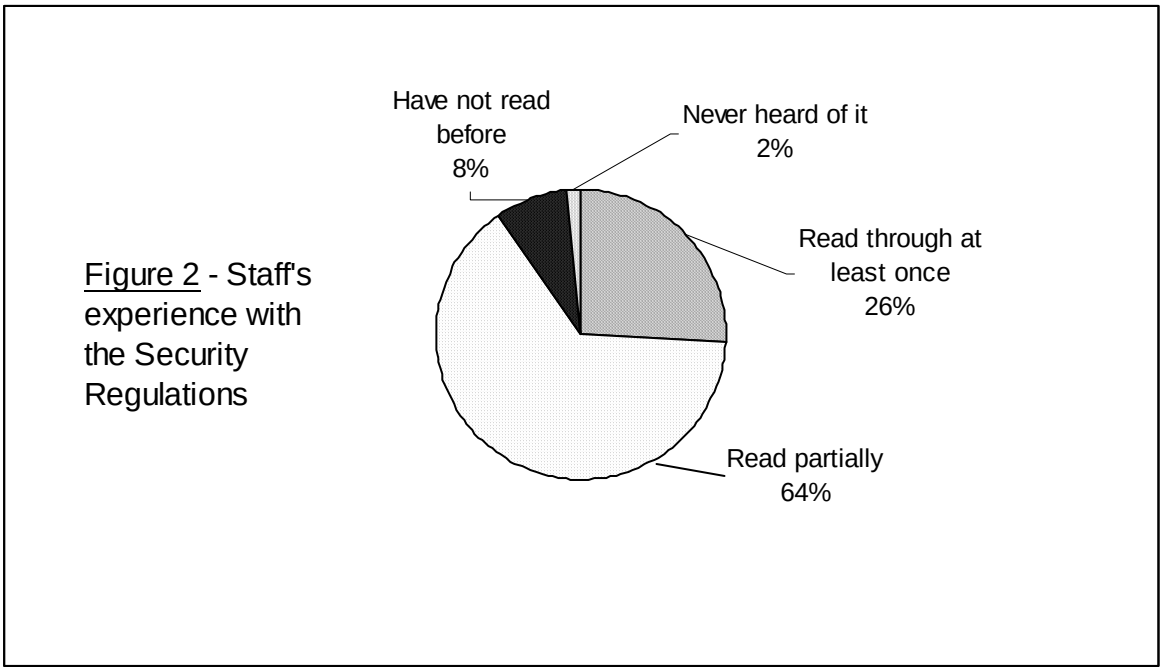


Figure 2 - Staff's experience with the Security Regulations

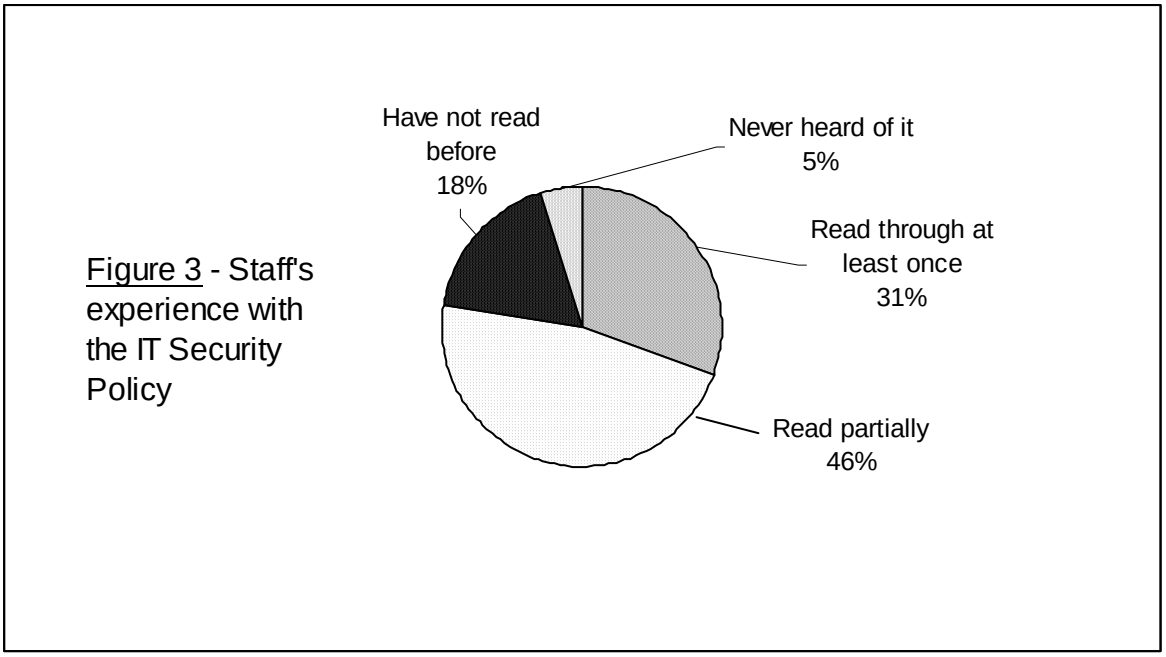


Figure 3 - Staff's experience with the IT Security Policy

4. On actual practices, staff in general are following the guidelines to protect their PCs and are adopting appropriate measures to protect data. The survey asked several questions about the staff's adopted security measures reflecting on their habit thus inference of their commitment in information security. **Figure 4** shows that nearly 80% of surveyed staff will often or very often activate the password for the screensaver before he/she leaves the computer. Also as indicated in **Figure 5**, nearly 80% will often check if any classified printouts are left unattended on the printer.

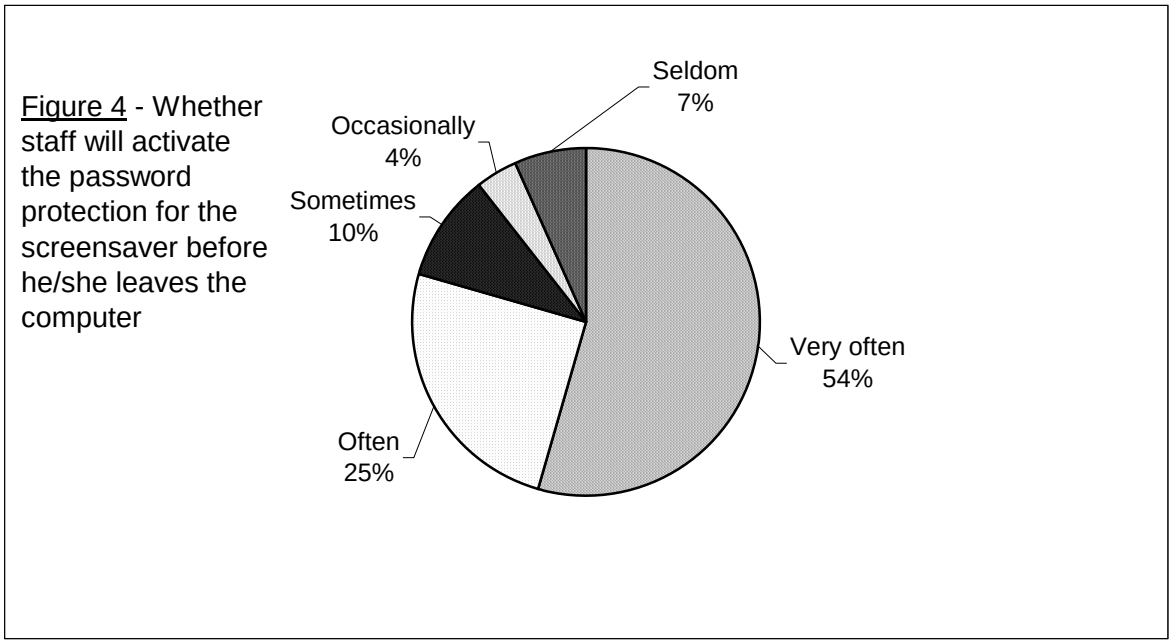


Figure 4 - Whether staff will activate the password protection for the screensaver before he/she leaves the computer

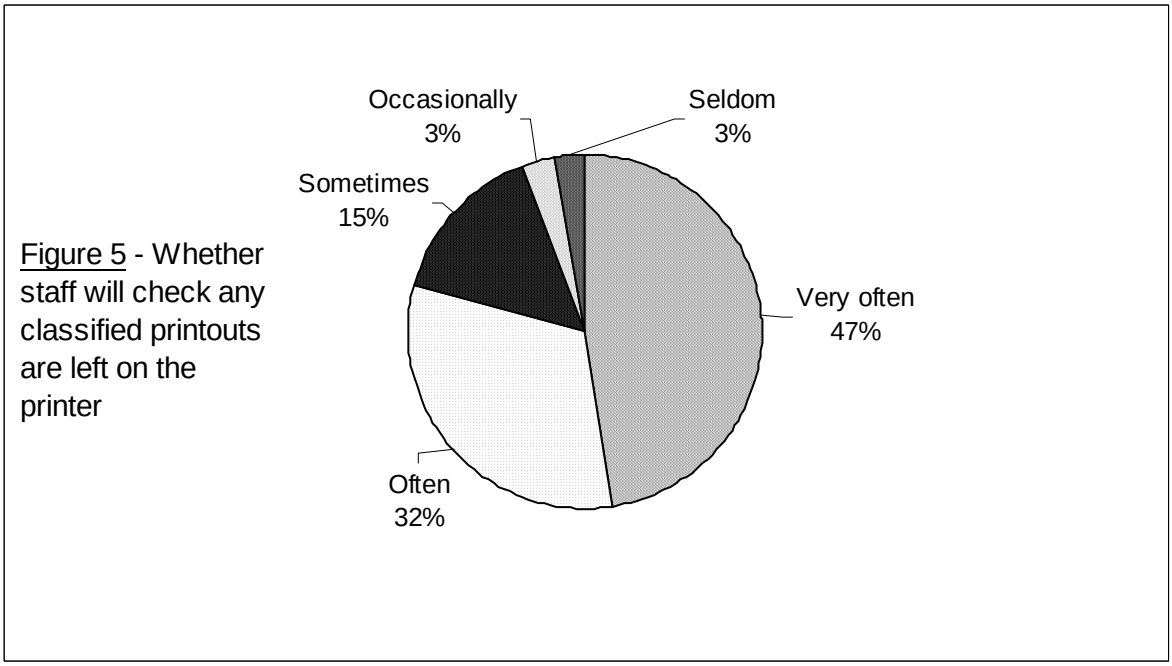


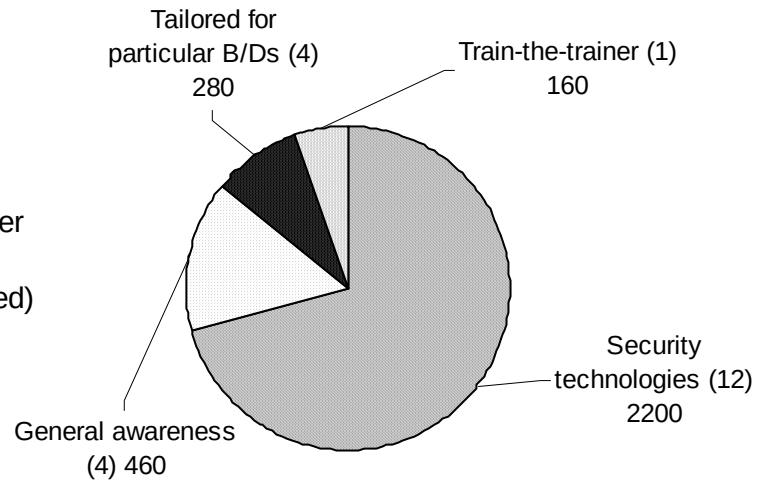
Figure 5 - Whether staff will check any classified printouts are left on the printer

Annex 2

ITB Panel Meeting on 13 July 2009

Training, seminars and related activities on Information Security June 2008 - May 2009

Figure 6 - Participants in trainings and seminars by category (number in bracket are events conducted)



In the past 12 months, the centre conducted or supported the conduct of more than 20 classroom training sessions and seminars to more than 3,000 staff from various B/Ds.

Annex 3

ITB Panel Meeting on 13 July 2009

Security Risk Assessment for the Hong Kong Police Force

The Government has conducted a service-wide information security audit to provide an independent assessment of the security compliance status of all bureaux and departments (B/Ds). The security audit exercise for the Hong Kong Police Force (HKPF) was carried out between December 2008 to May 2009 by an independent auditor under the management of the Office of the Government Chief Information Officer (OGCIO). The following paragraphs summarise the outcome and findings of this exercise.

2. The audit showed that HKPF has duly implemented security measures to protect their data and systems according to the security requirements. It has complied with security requirements in all the domain areas being audited, including outsourcing security, equipment security, access control security, data security and network and communication security.

3. The auditor had conducted interviews with relevant personnel, reviewed HKPF's security policy, procedures and settings, inspected supporting documentation such as reports, forms and emails, conducted site visit to the data centres and computer rooms, and carried out sample audit in selected critical systems.

4. On the use of portable electronic storage devices, the auditor found that HKPF had implemented stringent controls. As a departmental policy, all portable electronic storage devices for storing classified/personal information must be provided by HKPF, and use of privately owned portable electronic storage devices is prohibited.

5. To prevent accidental data leakage through the use of improperly configured software, HKPF does not allow the installation of any

unauthorised software. There is no Peer-to-Peer (P2P) file sharing software employed in their business operations.

6. The process and outcome of the Security Risk Assessment regularly arranged by HKPF were also studied during the audit. The results were positive in terms of the quality of activities in pre-assessment process, assessment process, assessment report and follow-up actions. HKPF has been following closely on the requirement issued by OGCIO on conducting security risk assessment.

7. A number of critical systems in HKPF had been selected for closer study. The security risk levels of these systems were found to be reasonably low. The audit did not expose any risk and the auditor only made minor suggestions to HKPF to further improve on certain areas, in particular:

- enhancing the process of conducting periodic or spot-check audit trails;
- enhancing IT asset inventory list record management; and
- examining a holistic approach for minimising the chances of taking out classified information from the office.

8. Despite HKPF's compliance status, there were still a number of data leakage incidents during early 2009. That might be due to insufficient awareness on information security of the concerned individuals. To address the risk factor of staff lacking awareness of the importance of safeguarding classified and personal data, HKPF has provided regular internal training/briefing, external training/briefing, e-learning courses, periodic reminders to their staff. Awareness training courses including data privacy training, information security training and Train-the-Trainer programme have been provided to different levels of staff.

9. OGCIO will follow up with HKPF on the areas of improvement as recommended by the auditor. As required by the Government's security policy, HKPF will regularly arrange security risk assessment conducted by external auditors on their applications and systems to ensure they can meet a high standard of security requirements.

Annex 4

ITB Panel Meeting on 13 July 2009

Summary of data leakage incidents in Government in the first two quarters of 2009

No.	Incident Date	Bureau/Department	Summary of the Incident and follow-up measures
1	January 2009	Food and Environmental Hygiene Department (FEHD)	An USB drive belonging to an officer in FEHD was found left in a public bus. The USB contained working documents and personal data of 103 citizens. FEHD subsequently notified and apologised to all affected individuals. The case was reported to the Privacy Commissioner for Personal Data.
2	January 2009	Hong Kong Police Force (HKPF)	An officially provided USB flash drive containing some internal information and personal data of 26 citizens was reported lost. The stored data was protected by strong password and AES 256-bit encryption to prevent access to the data stored therein.
3	February 2009	FEHD	Staff appraisal information relating to a FEHD staff was found through Foxy on the Internet. FEHD confirmed that the leaked document was an incomplete appraisal form of one Non-civil Service Contract staff and had apologised to the appraisee. Privacy Commissioner for Personal

No.	Incident Date	Bureau/Department	Summary of the Incident and follow-up measures
			Data had not been informed as only the names and posts of the appraisee and appraising officer but no other personal data were disclosed.
4	February 2009	Fire Services Department (FSD)	A number of documents including 32 staff appraisal reports and some internal information of FSD were found through Foxy. Personal data of 58 staff of FSD were involved. FSD had informed all affected individuals as well as the Privacy Commissioner for Personal Data.
5	February 2009	HKPF	Some internal information of HKPF was searchable through Foxy. The information was a template file for preparing statements of street gambling cases. Neither personal data nor information of any particular case was involved.
6	March 2009	HKPF	Some internal documents of HKPF dated from 2004 to 2008 were searchable through Foxy. The information included personal data of 60 staff and 36 citizens. HKPF had informed affected individuals as far as practicable and reported to the Privacy Commissioner for Personal Data.

Annex 5

ITB Panel Meeting on 13 July 2009

Progress of Actions taken by the Hospital Authority

Purpose

This note briefs Members on the progress of actions taken by the Hospital Authority (HA) since last meeting on 8 December 2008 regarding the privacy incidents in 2008, as well as the findings and recommendations to strengthen information security and privacy for patient data protection.

Background

2. The HA Task Force and the Privacy Commissioner for Personal Data (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. Corresponding action plans were developed to address the issues and recommendations within 18 months.

Action Plan and Progress

3. At the Administrative and Operational Meeting of the HA on 10 September 2008, the HA Board endorsed the proposed action plans for addressing the recommendations from Task Force and PCPD to further enhance protection of patient data security and privacy. The action plan with 19 consolidated targets covers the eight areas as mentioned in paragraph 2 above.

4. The following summarises further key actions that have been taken:

(a) In collaboration with PCPD, a privacy awareness campaign has been kick-started in May 2009 for all hospitals and targeted to all HA staff

aiming at raising the culture on privacy awareness via seminars and direct discussion with PCPD training officer. Further education programmes, including eLearning programs, have been developed to ensure that staff in the HA are adequately trained on the Personal Data (Privacy) Ordinance, policy and practical guidelines to protect patient personal data.

(b) The Corporate Information Security and Privacy Officer (CISPO) has been appointed and on board to take lead on Information Security and Privacy and oversee all corresponding initiatives of the HA-wide information security and privacy.

(c) Governance and organisation structures overseeing Information Security and Privacy in Head Office and in Clusters are established. The HA Information Security and Privacy Committee is in full operation to oversee all improvement works as detailed in the action plan.

(d) The HA wide information security and privacy policy has been reviewed, communicated and distributed for all HA staff highlighting the importance and principles of Information Security and Privacy.

(e) The information security and privacy compliance requirements on Clusters and outsource contractors has been established and incorporated.

(f) Accounts with access rights of downloading patient data are reviewed and reduced.

(g) PC security is further strengthened against data leakages and data downloading functions are further reduced and protected by encryption.

5. The remaining action plan targets involving policy and guideline reviews, compliance functions and other technology improvements will progressively be completed in 1Q 2010.

Hospital Authority
June 2009