LC Paper No. CB(1)2407/10-11(05)

For Information
on 13 June 2011

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 and changes in security posture since the last update on 12 July 2010.

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 updates provided in this paper cover three main areas –

(a) information security global trend;
(b) information security initiatives and posture in the Government; and
(c) information security in the wider community.

Information Security Global Trend

3. Today we are living in an environment where people and businesses are heavily reliant on information technology (IT) and the Internet. While enjoying the mobility, flexibility and efficiency, we also need to realise that there are corresponding security risks and threats. Cyber security is vital for citizens to protect their private data, for organisations to conduct their business securely, and for Government to provide public services in a trustworthy manner. Somehow threats such as

virus and worms, malicious code, identity theft and phishing attacks are continuous issues of concern to businesses and their customers. These security threats may strain the mutual trust between enterprises and their customers if the systems used and services provided are not robust enough to protect the availability, integrity and confidentiality of data.

4. With the proliferation of mobile devices and increased wireless connectivity, there are threats especially associated with mobile devices, such as notebook computers, consumer devices (e.g. tablet computers and smart phones), and portable storage devices (e.g. USB flash drives). There are risks of both external hackers who break through security perimeters and internal staff who do not take good care of an organisation's valuable or sensitive information. The advent and popularity of social networks may further increase the chance of information flow outside an organisation's network. Indeed, from time to time, there are news reported worldwide about massive leaks of information held by renowned organisations including some major platform providers.

5. The Government has the vision of maintaining a secure information and communications technology (ICT) environment for developing Hong Kong into a leading digital city. Our missions are therefore to uphold Government's information security policies and practices and develop a strong culture of data protection, as well as to promote information security to the public on the ethical use of IT facilities and proper ways to protect their computer resources and information assets. The Office of the Government Chief Information Officer (OGCIO) keeps track of the global trends of ICT development and closely monitors potential and actual cyber attacks with a view to advising B/Ds and citizens on necessary safeguards and aversion measures.

Information Security Initiatives in the Government

6. The OGCIO continues to promote the awareness of information security amongst staff, implement technical solutions against cyber security threats, and ensure proper governance and robust security management systems and practices are adopted by B/Ds to protect Government's IT assets, data and information. Various information

security initiatives for improving staff awareness and education; enriching technical and procedural measures; and strengthening compliance checking are presented in the following paragraphs.

(i) Staff Awareness and Education

7. Our staff awareness and education activities are ongoing. Awareness and education are considered to be the major contributing factors to enhance information security in B/Ds. In 2010-11, the OGCIO organised 10 security awareness seminars[1] with over 1 100 government staff attended. We also arranged 50 training courses (including those convened in-house or through external providers) for attendance by about 500 government staff. There are also over 50 sets of web-based training materials, more than 20 best practices, as well as a variety of thematic articles in the quarterly staff newsletters accessible on the Government Intranet. These resources aim to be beneficial for different levels of staff in the Government.

8. The security seminars and training courses centrally organised by the OGCIO were very well received by B/Ds[2]. Through the seminars and training courses, we provided security knowledge and technical know-how to the audience and reinforced their awareness on data protection. In 2011-12, the OGCIO will organise seminars covering topics of concerns to B/Ds including handling of classified information, business continuity and disaster recovery planning, identity management and access control, as well as threats associated with mobile computing, social networking and cloud computing. Staff acquiring formal training is also beneficial to B/Ds for carrying out security initiatives. Currently there are over 180 professional security certifications acquired by staff serving in various B/Ds.

[1] Security seminars covered a variety of topics including “Protection of the Confidentiality, Integrity and Availability of Sensitive Data”, “Good Security Habits”, and “Ensuring Your Security Strategy is Solid”.

[2] In a survey conducted in March – April 2011, over 90% of all B/Ds agreed the security training courses centrally organised by the OGCIO are useful for their staff, and they will continue to nominate staff to such training courses in future.

(ii) Technical and Procedural Measures

9. The OGCIO continues to carry out surveillance on risks associated with ICT development trends and identify security solutions available in the market to mitigate the risks. Through the Government Intranet, examples of security solution are provided to B/Ds for them to consider and implement in protecting their IT assets, data and information. Based on their business and operating requirements, B/Ds have been proactively adopting various security solutions such as portable storage devices with built-in encryption capability, patch management solutions, secure remote access solutions, etc. In view of increased usage of mobile computing gadgets, B/Ds adopt control measures such as enabling of password-protection features, allowing only use of authorised software, encrypting information during transmission or when in storage. When implementing wireless networks, B/Ds employ security controls such as protecting the access points, using strong encryption algorithm as stipulated in the latest industry standards, and separating internal wired network from the wireless network to prevent hacking.

10. The OGCIO issues security and virus alerts as soon as there are new vulnerabilities to remind B/Ds for taking timely actions to apply patches to fix software vulnerabilities, and follow security best practices in managing and operating their IT systems. For example, in the past six months, we issued over 30 security alerts and three reminders to keep B/Ds aware of the various security topics covering protection of mobile devices against malicious software and virus infection, protection from security threats of fraudulent websites and phishing attacks, and measures to protect government data and information systems. All B/Ds are also advised to share these resources with the public organisations and regulatory bodies under their purview.

(iii) Compliance Checking

11. According to the prevailing IT Security Policy, B/Ds are required to conduct security risk assessment and audit (SRAA) every two years, and follow up with the findings and recommendations arising from the SRAA. Starting from January 2011, we have strengthened the compliance

checking mechanism by requiring B/Ds to submit the SRAA results to the OGCIO within 6 months upon the completion of each exercise. This will enhance the governance level on one hand, and at the same time enable the OGCIO to have an overall understanding of the common pitfalls faced by B/Ds and their corresponding resolution measures. The centrally managed sample security audit conducted by OGCIO had also commenced in April 2011 and we target to complete 10 – 15 audits for each of 2011-12 and 2012-13. Additionally, periodic surveys will be conducted for all B/Ds to understand their plans, practices and actions related to information security and the one just completed was conducted from March to April 2011. The information collected through the above strengthened mechanism will be analysed for monitoring B/Ds' compliance status and designing security programmes in the long run. The audits have just started, and results will be progressively available towards the latter half of 2011.

Information Security Posture in the Government

12. Cloud Computing[3] is a global trend affecting the IT industry from both the supplier and user angles. The adoption of Cloud Computing in the provision of central IT services has been set out as a key theme of the government IT strategy. OGCIO is assessing the associated security risks to determine the most appropriate deployment option, with due consideration to availability, reliability, integrity, confidentiality and privacy. We will develop best practices and guidelines for sharing with B/Ds for their consideration in the adoption.

13. Keeping in pace with emerging security threats, new business initiatives, use of new technologies and service models, and changing user behaviors on the Internet remain challenging. For the period July 2010 to May 2011, there have been five cases of data leakage reported to the Government Information Security Incident Response Office[4] (GIRO) which had shown signs of decreasing[5]. Of these five cases, two involved loss of USB flash drive, two others were related to documents searchable

[3] Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[4] The GIRO comprises members from the OGCIO, Security Bureau and the Hong Kong Police Force.

[5] The number of data leakage cases reported to the GIRO in the 12-month periods of July 2008 to June 2009 and July 2009 to June 2010 were 9 and 8 cases respectively.

on the Internet and one was related to a computer programming error. For cases involving personal data, B/Ds have submitted reports to the Office of the Privacy Commissioner for Personal Data (PCPD) and notified the affected individuals as appropriate. Details of these cases are in **Annex**.

Information Security in the Wider Community

14. For the community, the OGCIO continues to organise different events in collaboration with industry and professional bodies to enhance public awareness of the need and knowledge to protect their computer resources and information assets. In 2011, we continue to collaborate with stakeholders including Hong Kong Police Force (HKPF) and Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) to organise three public seminars for the general public and a symposium for industry players including Internet Service Providers (ISPs). Given the increasing trend of security threats on the mobile platforms and the popularity of social networking, the topics to be covered will focus on security trends and issues related to mobile devices, social networking and fraudulent online transactions. For the ISP symposium, there will be a session on cyber attack and mitigation measures.

15. The OGCIO publishes security related news reported in Hong Kong and overseas in our information security portal (www.infosec.gov.hk) to keep the public apprised of emerging security issues that may affect them. Starting from April 2010, we have broadcast a new series of radio episodes on RTHK with a thematic title every month providing the public with tips and best practices on information security (e.g. protection against data leakage, safe social networking and mobile security). We also share training videos and flash animations used in the government staff training programmes with the general public through the information security portal to enhance information security awareness in the community. In the 2010 “Hong Kong Clean PC Day” campaign[6], we convened a logo design contest with overwhelming response from 280 contestants. The award was presented in November 2010.

[6] The “Hong Kong Clean PC Day” is an annual promotion campaign on information security jointly organised by the OGCIO, HKCERT and HKPF.

16. To test the coordination amongst local Internet infrastructure stakeholders during major incidents, an information security incident response drill was coordinated by the HKCERT and participated by relevant parties[7] in October 2010. Through the exercise which was held the second time, the participants gained experience on how to respond to emergency conditions and the organiser gained insightful inputs on how to coordinate and improve communication amongst the stakeholders during major incidents.

Conclusion and Next Steps

17. Nowadays, security threats become even more diversified covering mobile devices and services, social networking, identity theft, etc. The Government will continue promoting the awareness and alertness of information security in the community, maintaining close surveillance on cyber security threats, and ensuring proper governance and robust security management systems and practices are adopted by B/Ds. Given that information security is an ongoing process, we will continue to implement various security initiatives to safeguard Government’s IT assets, data and information.

Advice Sought

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

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau
June 2011

[7] Participants included the OGCIO, HKPF, Hong Kong Internet Service Providers Association, Hong Kong Internet Exchange, Hong Kong Internet Registration Corporation Ltd, the DotAsia Organisation, etc.

Annex

Summary of data leakage incidents in Government from July 2010 to May 2011

No.	Incident Date	Bureau/ Department	Summary of the Incident and follow-up measures
1	July 2010	OGCIO	A staff member of the S.K.H. Holy Carpenter Church Community Centre (HCC) who was engaged by OGCIO to implement the "Be NetWise" Internet Education Campaign at the Kowloon City district lost a USB flash drive containing personal data of total 4,413 participants of activities conducted by the HCC. The case was reported to the PCPD and all affected individuals were informed.
2	November 2010	Labour Department (LD)	An email notification program in the Interactive Employment Service (iES) website of LD sent out emails with sensitive information of 220 registered users to unintended recipients. It was confirmed that no data was modified during the incident period. The case was reported to the PCPD and all affected individuals were informed. The program bug was identified and fixed.
3	February 2011	HKPF	Three documents allegedly belonged to the HKPF were searchable on the Internet. One document was a previously leaked statement containing personal data. The second document was an unclassified document publicly available on HKPF's website. The third document was an obsolete version of rules in using police firearms. No personal data of new individual was involved.

No.	Incident Date	Bureau/ Department	Summary of the Incident and follow-up measures
4	April 2011	HKPF	Four documents allegedly belonged to the HKPF were searchable on the Internet. Investigation was still in progress to ascertain the source of leakage. One document was believed to be a draft application form for Inspector of Police prepared by a citizen, which was not leaked by the HKPF. The other three documents were believed to be leaked through privately-owned computer via FOXY. Personal data of 17 individuals, including 15 Police officers and two citizens were involved. The case was reported to the PCPD and all affected individuals were informed.
5	May 2011	Social Welfare Department (SWD)	A staff lost a privately-owned USB drive containing personal particulars including name and ID number of two individuals. The case was reported to the PCPD and all affected individuals were informed.