立法會
Legislative Council

LC Paper No. CB(4)797/12-13(01)

Ref. : CB4/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 8 July 2013

Updated background brief on information security

Purpose

This paper gives a summary of views and concerns raised by Members during previous discussions on Government's information security programmes.

Background

2. People and businesses nowadays are heavily reliant on information technology ("IT") and the Internet. While enjoying the mobility, flexibility and efficiency, the community also needs to realize that there are corresponding security risks and threats. In this regard, the Government has endeavoured to enhance the security measures in bureaux/departments ("B/Ds") and provide support to the community for improving their information security status in the following 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. Cyber security is essential for citizens to protect their private data, for organizations to conduct their business securely, and for the Government to provide public services in a trustworthy way. Somehow threats such as virus

and worms, malicious code, identity theft and phishing attacks are continuous issues of concern to businesses and their customers. The Office of the Government Chief Information Officer ("OGCIO") is responsible for keeping track of the global trends of information and communications technology ("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 and posture in the Government

4. Within the Government, OGCIO is responsible for promoting the awareness of information security amongst Government 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.

5. Cloud Computing has become 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 and developing best practices and guidelines for sharing with B/Ds for their consideration in the adoption.

Information security in the wider community

6. OGCIO organizes 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. It also publishes security related news reported in Hong Kong and overseas in its information security portal (www.infosec.gov.hk) to keep the public apprised of emerging security issues that may affect them.

Previous discussions

7. At the meeting of the Panel on Information Technology and Broadcasting ("the Panel") on 13 June 2011, members noted the launch of the "International Strategy for Cyberspace" by the Government of the United States in May 2011, and urged the Administration to enhance its own information security posture and formulate a comprehensive strategy against large scale attacks on Government and other websites in the Cyberspace. The Administration advised that it would assess the impact of online attacks on Hong Kong, and review the information security posture. An ongoing communication mechanism was set up amongst OGCIO, the Security Bureau

and the Hong Kong Police Force ("HKPF") and any findings relevant to Hong Kong would be shared with the concerned B/Ds.

8. Panel members noted that data leakage incidents were commonly related to the use of the Foxy software and the loss of USB flash drives. They raised concerns about the Administration's strategy to prevent the recurrence of similar incidents. The Administration advised that OGCIO continued to carry out surveillance on risks associated with ICT development trends and identify security solutions available in the market to mitigate the risks. Based on their operating requirements, B/Ds had been proactively adopting various security solutions recommended by OGCIO such as portable storage devices with built-in encryption capability. B/Ds also adopted control measures such as implementing software asset management that allowed only use of authorized software, and enhanced staff awareness and education in information security.

9. Panel members also noted that the Administration had contracted out the overall coordination of computer security incident response for local enterprises and Internet users to the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) managed by the Hong Kong Productivity Council. Members opined that adequate funding should be provided to HKCERT for upgrading their IT infrastructure which had become outdated and were unable to keep abreast of information security requirements. The Administration advised that HKCERT would submit annual service proposal with the corresponding information security resource requirements to OGCIO for consideration. Besides HKCERT, OGCIO maintained a good co-ordination network with Internet infrastructure stakeholders and related parties, including the Security Bureau, HKPF, the former Office of the Telecommunications Authority (now known as "Office of the Communications Authority[1] ") and the Internet service providers, to safeguard the integrity of the Internet infrastructure, to conduct 24-hour surveillance on Internet incidents on a need basis and to ensure that emergency response work would be carried out effectively.

10. At the Panel meeting on 10 July 2012, members noted the 40 fold increase in incidents of global intrusion of mobile platform and the service disruption incident on the platforms of a local telecommunications service provider. Some members urged the Administration to step up measures to enhance the information security posture of the local service providers and the incident reporting system. These members also urged the Administration to promote the awareness of information security in small and medium enterprises ('SMEs") and the wider community. OGCIO advised that according to the findings of the incident report submitted by the telecommunications service

---

[1] Pursuant to the Communications Authority Ordinance (Cap 616), with effect from 1 April 2012, all duties and powers of the Telecommunications Authority are conferred on the Communications Authority (CA), and all duties and powers of the OFTA are conferred on the OFCA, the executive arm of the CA.

provider concerned to the CA, the incident on 29 June 2012 was caused by a software bug in the system rather than a malicious attack resulting in the temporary degradation of the 3G mobile data service. To promote the adoption of security best practices in the telecommunications business and the wider community, OGCIO published security best practices on its thematic website (www.infosec.gov.hk) and organized seminars and publicity campaigns on information security in collaboration with the HKCERT.

Recent developments

11. At the special meeting of the Finance Committee on 10 April 2013, Hon Charles Peter MOK enquired whether the Administration had any plan to promote and implement the information security policies and guidelines with other B/Ds. He also enquired about the specific measures taken in 2013-2014 to promote public awareness and education in the face of increasingly serious information security threats, and the resources required for implementing these measures. The Government Chief Information Officer's replies are in **Appendices I** and **II**.

12. At the Council meeting of 5 June 2013, Hon Andrew LEUNG raised a question on promoting use of ICT amongst SMEs. He also urged the Administration to help SMEs understand and remove the potential risks in information security of cloud computing. The Administration advised that the Government had been disseminating up-to-date reference materials and news on information security via various channels, including the "InfoSec" portal, talks, seminars and publicity leaflets/pamphlets, to help SMEs understand various security risks and the necessary security measures. The Government also published materials on information security, including the "Security & Privacy Checklist for Cloud Service Providers in Handling Personal Identifiable Information in Cloud Platforms" and "Security Checklists for Cloud Service Consumers" through the above-mentioned portal for reference by SMEs. When formulating information security guidelines, the Government had made reference to international standards on information security and industry guidelines.

13. On the recommendation of the House Committee at its meeting on 14 June 2013, the President has given permission for Hon MA Fung-kwok to ask an urgent oral question under Rule 24(4) of the Rules of Procedure ("RoP") at the Council meeting of 19 June 2013 relating to allegations of hacking into computers in Hong Kong by the government of the United States. The President has also given permission for Hon Andrew LEUNG to move, under Rule 16(4) of the RoP, a motion for adjournment at the said Council meeting. The wording of the motion is as follows:

"That this Council do now adjourn for the purpose of debating the following issue: cyber security."

Latest position

14. The Administration will brief the Panel on 8 July 2013 on the progress and development of Government's information security programmes.

Relevant papers

15. A list of the relevant papers with their hyperlinks is at:
http://www.legco.gov.hk/yr11-12/english/panels/itb/papers/itb_fs.htm
http://www.legco.gov.hk/yr12-13/english/fc/fc/w_q/cedb-ct-e.pdf
http://www.info.gov.hk/gia/general/201306/05/P201306050598.htm

Council Business Division 4
Legislative Council Secretariat
18 June 2013

Examination of Estimates of Expenditure 2013-14

Reply Serial No.

CEDB(CT)106

CONTROLLING OFFICER'S REPLY TO INITIAL WRITTEN QUESTION

Question Serial No

3214

Head: 47 – Government Secretariat : Office of the Government Chief Information Officer

Subhead (No. & title):

Programme: (2) IT Infrastructure and Standards

Controlling Officer: Government Chief Information Officer

Director of Bureau: Secretary for Commerce and Economic Development

Question: Regarding the review of government information security related regulations, policies and guidelines, would the Administration inform the Committee of the following:

(a) time-table for follow-up actions;

(b) specific details of expenditure reserved for the relevant arrangements; and

(c) whether it has any plan to promote and implement the guidelines with other bureaux/departments? If so, what are the manpower and resources required?

Asked by: Hon. MOK, Charles Peter

Reply: The Office of the Government Chief Information Officer (OGCIO) promulgated the revised information security policies and guidelines to all bureaux and departments (B/Ds) in September 2012, and conducted a briefing session to explain and promote the revised information security requirements to officers responsible for information security in B/Ds in November 2012. Apart from internal promulgation, the revised policies and guidelines are also published on the thematic information security portal (www.infosec.gov.hk) for public reference.

(a) The revisions mainly require B/Ds to strengthen protection of government systems and information. B/Ds are required to implement measures to ensure that their information systems are in compliance with the revised information security policies and guidelines. They are also required to conduct periodic security risk assessment and audit on their information systems to ensure that the security requirements are met.

(b)&(c)

OGCIO and the Security Bureau will arrange refresher training for Departmental Information Technology (IT) Security Officers of all B/Ds in mid-2013, and will assist B/Ds in implementing information security programmes with appropriate control measures. The IT security team of OGCIO will undertake the promotion work and will assist B/Ds in implementing the guidelines. The team, comprising 9 staff members, is responsible for the central coordination on information security matters and carrying out promotion and education activities. The estimated expenditure for 2013-14 is about $5.8 million. The manpower and expenditure involved will be absorbed by the budget provision of OGCIO in 2013-14. No additional resources and

manpower are required. Moreover, the annual project expenditure of conducting random audit check for 15 B/Ds by OGCIO is about $1.8 million, which is met under Head 710 Computerisation of the Capital Works Reserve Fund.

Name in block letters: Daniel LAI

Post Title: Government Chief Information Officer

Date: 8.4.2013

Examination of Estimates of Expenditure 2013-14

Reply Serial No.

CEDB(CT)107

CONTROLLING OFFICER'S REPLY TO INITIAL WRITTEN QUESTION

Question Serial No

3215

Head: 47 – Government Secretariat : Office of the Government Chief Information Officer

Subhead (No. & title):

Programme: (3) IT in the Community

Controlling Officer: Government Chief Information Officer

Director of Bureau: Secretary for Commerce and Economic Development

Question: In the face of increasingly serious information security threats, what specific work will be commenced by the Government in 2013-14 to promote public awareness and education on information security? How much resources are expected to be allocated in this regard as compared with 2012-13? What are the specific work objectives, details of plan and time-table of the promotion and education activities conducted for government departments, public organisations, educational institutions, small and medium enterprises and business corporations?

Asked by: Hon. MOK, Charles Peter

Reply: Today we are living in an environment where citizens and businesses are heavily reliant on information technology (IT) and the Internet. Ensuring cyber security is vital for citizens, organisations and the Government. In this respect, the major work of the Office of the Government Chief Information Officer (OGCIO) is to continuously promote information security to the public, raise their awareness on the appropriate use of IT facilities, and assist them in adopting proper ways to protect their computer resources and information.

OGCIO disseminates references and information on information security to the public (including small and medium enterprises (SMEs)) through various promotion channels, including the InfoSec portal, seminars, radio, information leaflets and pamphlets. Through collaboration with the Hong Kong Police Force and the Hong Kong Computer Emergency Response Team Coordination Centre, OGCIO holds an annual campaign of promotion events staged throughout the year to address concerned issues on information security. In addition, OGCIO has all along been supporting the industry and professional bodies to organise information security activities. In 8 public seminars on information security held by local industry and professional bodies in 2012-13, OGCIO had either acted as a supporting organisation or sent designated representatives to speak at the seminars, conveying messages on information security and providing relevant advice to the public.

In 2013-14, we will continue to organise various events including 4 public seminars and 1 video contest under the theme "Build a Secure Cyberspace". Through these activities, we aim to raise the awareness of information security among organisations and citizens, and strengthen the protection of personal computers and IT facilities against cyber attacks. Moreover, we will, in collaboration with professional bodies, visit about 10 schools to promote the knowledge of Internet safety to teachers and students. We will also continue to cooperate with the Radio Television Hong Kong to produce audio clips with different topics every month, providing practical tips and security best practices on information security to

citizens. To facilitate the public and enterprises (particularly SMEs) in accessing information and resources on cloud technologies effectively, the Expert Group on Cloud Computing Services and Standards (comprising representatives from OGCIO, the industry, the academia and professional bodies) has set up a one-stop portal (InfoCloud) to provide sample use cases, relevant guidelines and best practices for reference by the public and enterprises to enable them to achieve the intended benefits in adopting the cloud model. Internally, we will hold 4 seminars for bureaux and departments (B/Ds) and will arrange refresher training for Departmental IT Security Officers of all B/Ds to enhance their awareness and knowledge on information security.

The IT security team of OGCIO, comprising 9 staff members, is responsible for the central coordination on information security matters and carrying out the above promotion and education activities. The total expenditure incurred by the IT security team in 2012-13 was around $5.34 million and the estimated expenditure for 2013-14 is about $5.8 million. The manpower and expenditure involved have included the resources required for carrying out the above promotion activities by OGCIO.

Name in block letters: Daniel LAI

Post Title: Government Chief Information Officer

Date: 8.4.2013