立法會

Legislative Council

LC Paper No. CB(1)2305/11-12(06)

Ref. : CB1/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 10 July 2012

Updated background brief on information security

Purpose

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

Background

2. People and businesses nowadays are heavily dependent 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 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. It will develop 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. Members have followed up the issue of information security since 2008. Views and concerns raised at meetings of the Panel on Information Technology and Broadcasting (the Panel) were summarized in the ensuing paragraphs.

Information security global trend

8. At the Panel meeting 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.

9. 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.

Information security in the Government and the wider community

10. At the Panel meeting on 13 June 2011, 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.

11. 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.

12. The Panel 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. Panel 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.

13. 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

[1] Pursuant to the Communications Authority Ordinance (Cap 616), with effect from 1 April 2012, all duties and powers of the Telecommunications Authority (TA) 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.

a need basis and to ensure that emergency response work would be carried out effectively.

Recent developments

14. At the special meeting of the Finance Committee on 7 March 2012, Dr Samson TAM enquired about the progress of the OGCIO review of Government information security related regulations, policies and guidelines which commenced in 2011-2012. The Administration advised that it was interviewing stakeholders, including management and operation staff responsible for information security in various B/Ds, to gather their views and suggestions. Reference would also be made to the information security policies of other economies. The Administration was also examining the impact of certain emerging information technologies, including cloud computing, mobile technology and social network, on the information security requirements. The Administration expected to complete the review and promulgate the revised government information security related regulations, policies and guidelines by the end of 2012.

Latest position

15. The Administration will brief the ITB Panel on the progress of Government's information security enhancement initiatives since the last update on 13 June 2011.

Relevant papers

16. 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

Council Business Division 1
Legislative Council Secretariat
4 July 2012