立法會
Legislative Council

LC Paper No. CB(4)1212/14-15(04)

Ref. : CB4/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 17 July 2015

Updated background brief on information security

Purpose

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

Background

2. The objectives of the Government's information security programmes are to formulate and implement information security policies and guidelines for compliance and reference by bureaux and departments ("B/Ds"), ensure that all the Government's information technology ("IT") infrastructure, systems and information are secure and resilient, and promote and enhance the awareness of information security and cyber risks among organizations and members of the public in the following three main areas:

(a) information security threats and risks;
(b) information security measures in the Government; and
(c) information security in the wider community.

3. As an active participant in the cyber space, it is important for all stakeholders, including the Government, businesses and the public, to understand the associated risks and learn the skills to protect their information systems and sensitive data. The Government keeps abreast of global information security trend and development at all times. Through the one-stop InfoSec portal (www.infosec.gov.hk), reference information and latest security

news as well as measures and best practices for prevention of cyber crimes are provided to raise the awareness of enterprises and citizens on the importance of information security. The Administration has also been distributing security alerts and warnings through emails and the GovHK Notifications mobile application.

4. Within Government, the Administration monitors security threats and technology trends to introduce appropriate protection measures to safeguard government IT systems and information assets. In 2013-2014, the Administration issued 63 high-threat security warnings and four security reminders to alert government users on prevailing or imminent security threats and advise them to take appropriate follow-up actions. The Administration had also revised the Government's incident response mechanism to strengthen the incident response life cycle management to require all B/Ds to strictly follow the incident response requirement in prioritizing resources to react to identified security events and implement appropriate remedial actions.

5. In facing the increasing trends of cyber threats and the potential public impact of targeted attack to government information systems and data assets, within Government, a task force comprising representatives from the Office of the Government Chief Information Officer ("OGCIO"), the Security Bureau ("SB") and the Hong Kong Police Force ("HKPF") had started to review the existing computer emergency response and incident handling management framework in the Government with a view to strengthening the cyber security capabilities. The task force will make reference to the best practices in other governments and recommend enhancement measures to strengthen the computer emergency response capabilities in the Government.

6. In the community, the Hong Kong Computer Emergency Response Team ("HKCERT") is the centre for coordination of computer security incident response for local businesses and individuals. HKCERT coordinates with Computer Emergency Response Teams in other places of the world to disseminate security alerts and warnings as well as provide advice on preventive measures against security threats. In 2013-2014, HKCERT published 443 security bulletins and 103 security blogs, increased from 439 and 78 respectively in 2012-2013. HKCERT has also published the "Hong Kong Security Watch Report" on a quarterly basis since the fourth quarter of 2013 to inform the public on the latest trends of identified security events and areas of concerns with appropriate advice on preventive measures.

Previous discussions

Panel on Information Technology and Broadcasting

7. At the meeting of the Panel on Information Technology and Broadcasting ("the Panel") on 22 July 2014, some members noted the cyber attack in June 2014 on Project PopVote, a website established to gauge support for universal suffrage, and expressed concern whether follow-up actions had been taken by the Administration in the aftermath of the attack and whether any prosecutions had been taken against similar attacks in the past. These members also enquired about the channel for individual organizations to seek assistance in case of a cyber attack and measures taken by the Administration to guard against the emergence of cyber threats.

8. The Administration advised that having noted the media reports on the attack, it had taken the initiative of liaising closely with the stakeholders, including the Hong Kong Internet Registration Corporation Limited, the Hong Kong Internet Exchange of the Chinese University of Hong Kong and the Internet service providers, with a view to strengthening protection against cyber attacks on the critical infrastructures. In 2012, the perpetrator of a distributed denial-of-service attack against the Hong Kong Stock Exchange was convicted of accessing a computer with criminal or dishonest intent. In cases of cyber attacks, individual organizations could approach HKCERT for further assistance.

9. The Administration also advised that in 2012, HKPF had established the Cyber Security Centre to enhance protection of Hong Kong's critical infrastructures and strengthen Hong Kong's resilience capabilities against cyber attacks. HKPF planned to extend the roles and responsibilities of their existing Technology Crime Division to a new Cyber Security and Technology Crime Bureau in the latter part of 2014, with the objectives to strengthen HKPF's capabilities in protecting information systems of critical infrastructures, as well as meeting the various challenges of emerging technology crimes. HKPF would focus on investigation and prosecution and OGCIO would work proactively to promote awareness and education in information and cyber security, and collaborate with local and overseas stakeholders to strengthen the collection and sharing of security intelligence.

10. Noting media reports on hidden malicious software in mobile applications ("apps"), some Panel members opined that measures should be formulated to enhance information security in mobile devices. The Administration advised that it attached great importance to the security of mobile apps. In this regard, security tips for using mobile apps were

disseminated through the Government's InfoSec portal (www.infosec.gov.hk), a dedicated webpage of HKCERT, and seminars organized by OGCIO.

Finance Committee

11. At the special meeting of the Finance Committee on 30 March 2015, Dr Hon Elizabeth QUAT, Hon Charles Peter MOK and Hon SIN Chung-kai sought information on the existing Government policies, measures, facilities and financial resources to maintain the security of information systems of the Government and the community, and the results and expenditure on conducting security checking for government websites and web apps.

12. According to the Administration, OGCIO (in collaboration with SB) had formulated comprehensive information security policies, guidelines and procedures and all B/Ds were required to follow them strictly. B/Ds must implement appropriate and professional security measures, including the installation of firewalls, anti-virus solutions, intrusion detection and prevention systems, and security facilities to monitor, detect and block cyber attacks so as to protect the security of government information systems. Information security was a mandatory system requirement generally included in the development and maintenance of government information systems. Since the expenditure on information security was usually included in other costs related to the use of IT, there was no separate breakdown for the expenditure on information security.

13. In the community, the Administration advised that OGCIO maintained close contacts with HKCERT and industry associations to closely monitor the overall situation of network security in Hong Kong. It regularly organized promotional and educational activities to raise public awareness and knowledge of information security. HKCERT also provided services and information related to computer security incidents and information security solutions to local enterprises and members of the public for them to better maintain the security of their information systems. In 2015-2016, OGCIO would provide funding support of about $10 million to the Hong Kong Productivity Council for HKCERT to deliver its services. In addition, OGCIO had launched the Cyber Security Information Portal (cybersecurity.hk) in January 2015 with a view to raising public awareness and knowledge of information security. The estimated expenditure for the related promotional activities was around $0.28 million.

14. The Administration also advised that the expenditure for conducting security checking for government websites and web apps was about $3.2 million. Checking results revealed that the government websites and web

apps had generally implemented effective security measures and were able to guard against cyber attacks. To further enhance the protection capabilities of government internal information systems, thematic seminars and workshops were arranged to share the experience and results of the security checking with related government staff to keep them abreast of the security risks, technologies and solutions of websites and web apps and enhance their knowledge and capabilities to guard against cyber attacks.

Council meeting

15. At the Council meeting on 22 October 2014, Dr Hon Elizabeth QUAT raised question relating to the declaration of cyber war codenamed "Operation Hong Kong" in early October 2014 by an international hackers' group which threatened to hack into the websites of the Hong Kong Government and make public the Government's confidential information and personal data of officials. Subsequently, there were reports about local websites being attacked by hackers leading to temporary suspension of their network operation. Dr Hon Elizabeth QUAT enquired, inter alia, whether the authorities had comprehensively reviewed and enhanced the cyber security measures of various government departments since the declaration of cyber war, and about measures taken to ensure that public and private organizations, including individuals, would be protected from attacks by local or overseas hackers.

16. The Administration advised that the Government was aware that the hacker group had attempted to attack some Government websites, making those websites slow in operation by significantly increasing their traffic. OGCIO had worked with the relevant departments to take appropriate measures to block the intrusion and get the websites back to normal operation. With regard to cyber security, all B/Ds were following the standing information security policies, procedures and guidelines to protect Government information systems. Since the declaration of the cyber attack by the hacker group, OGCIO had immediately contacted and reminded B/Ds to examine their network security measures, strengthen defence, activate relevant contingency plans, as well as closely monitor the situation to ensure normal operation of Government computer systems.

17. The Administration further advised that it would collaborate closely with relevant stakeholders (including HKCERT) to address cyber attacks. Upon receipt of enquiries or incident reports, HKCERT would provide advice and support on IT security matters to those seeking help, and assist them in fixing the vulnerability and taking measures to guard against cyber attacks.

Latest position

18. The Administration will brief the Panel on 17 July 2015 on the progress and development of the Government's information security programmes.

Relevant papers

19. A list of the relevant papers with their hyperlinks is at:

http://www.legco.gov.hk/yr15-16/english/panels/itb/papers/itb_fs.htm
http://www.legco.gov.hk/yr13-14/english/panels/itb/minutes/itb20140722.pdf
http://www.legco.gov.hk/yr14-15/english/fc/fc/w_q/cedb-ct-e.pdf
http://www.info.gov.hk/gia/general/201410/22/P201410220495.htm

Council Business Division 4
Legislative Council Secretariat
9 July 2015