立法會
Legislative Council

LC Paper No. CB(4)577/17-18(04)

Ref. : CB4/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 12 February 2018

Updated background brief on information security

Purpose

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

Background

2. The objectives of the Administration'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 Administration'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.

3. The Administration has launched dedicated programmes to strengthen the security measures of its information systems and Internet infrastructures, and has collaborated with key stakeholders to raise public awareness and knowledge of information security through sharing best practices and guidelines. The developments of the Administration's information security programmes were summarized under the following three main areas:

(a) information security in the Government;

(b) information security initiatives in the wider community; and

(c) public awareness and education.

Information security in the Government

Preventive measures

Monitoring cyber risk trends

4. The Administration is committed to protecting its information infrastructure and data assets, and has implemented multiple layers of security measures to address increasing incidents of cyber attacks and related security threats within the Government. The Office of the Government Chief Information Officer ("OGCIO") collects cyber threat information issued by the cyber security industry and the Computer Emergency Response Teams ("CERTs") of other places, and disseminates timely security alerts and reminders to B/Ds and assists government IT staff and departmental emergency response teams in B/Ds to prepare for prompt response and strengthen their precautionary measures.

5. To strengthen the Government's capabilities on monitoring cyber threats and sharing relevant information, OGCIO employs big data analytics technology for establishing a cyber threat information sharing platform which can collect and analyze cyber threat information and data, detect potential incidents. This would allow more targeted cyber threat alerts to be provided to B/Ds, and would allow sharing of cyber risk information among the industry, businesses and the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT")[1].

Conducting risk assessment and follow-up

6. B/Ds has implemented security-related measures including conducting of security risk assessments and audits, implementation of technical security solutions and upgrading of security infrastructure. OGCIO carries out independent information security compliance monitoring and audits for all B/Ds. During the course of assessment, OGCIO assists relevant

[1] HKCERT is managed by the Hong Kong Productivity Council to coordinate computer security incident response for local enterprises and Internet users.

B/Ds in carrying out continued improvement to the security management systems and coping with emerging security threats.

Data protection measures

7. To ensure protection of government data assets, the Administration uses encryption with the highest industry standards when storing and transmitting sensitive data and documents. OGCIO has requested B/Ds to strengthen data protection and develop systems to enhance their capacities in monitoring, detecting and blocking data leakage in the Government. B/Ds are also requested to monitor and analyze, and if necessary, block suspicious data flow in their networks.

Denial-of-service attack

8. OGCIO assists B/Ds to implement appropriate protection measures and strengthen threat detection capabilities, including vulnerability scanning and penetration testing, against distributed denial-of-service and web defacement attacks. OGCIO also issues timely alerts and advisories to B/Ds to take management and technical measures to protect government websites and data.

Ransomware and malware attacks

9. From time to time, OGCIO issues high-risk security alerts and security reminders to B/Ds security guidelines related to ransomware, and reminds all staff not to open suspicious emails and their attachments and links to prevent their computers from being infected. OGCIO also reminds B/Ds to use anti-malware software regularly to scan their computer systems and perform data backup, and store the backup copy offline.

IT security policy and governance

10. The Administration has put in place the "Government IT Security Policy and Guidelines" ("the Guidelines") for compliance by B/Ds with a view to strengthening the compliance requirements and security practices to cope with different types of emerging threats, such as malicious attacks, data leakage, network intrusions and phishing attacks.

11. With reference to the latest version of ISO 27001 international standards and other industry best practices, the Administration has reviewed the Guidelines, including increasing the confidentiality requirements for storage of sensitive information, strengthening departmental management

capability for information security incident response, reviewing the capabilities of information security technology and detection of emerging cyber attacks, so as to address different types of information security threats and cyber attacks.

12. OGCIO conducts compliance audit for B/Ds on a regular basis to ensure their compliance with the Government IT security regulations, policies and requirements. It has formulated practical guidelines and security requirements regarding the use of external storage devices to transport government documents and facilitated B/Ds to adopt appropriate technologies for encrypting government data.

Training for government staff

13. Training has been arranged for support personnel to update their knowledge on emerging threats and technical skills to mitigate risks. In particular, OGCIO assists government IT staff and departmental emergency response teams in B/Ds to prepare for prompt response and strengthen their precautionary measures. OGCIO also organizes information security-related briefings, seminars and training workshops, etc., regularly for government staff at various levels to raise their security awareness, strengthen their knowledge on cyber attacks and the latest IT security technologies and solutions. These training sessions are also aimed at enhancing the information security skills of government staff, and thereby strengthen B/Ds' capabilities in guarding against such attacks and protecting the Government's information systems and sensitive information.

Collaboration within Government and with the industry

14. Through the Government Computer Emergency Response Team Hong Kong ("GovCERT.HK")[2], OGCIO collaborates with the Hong Kong Police Force ("HKPF") in organizing cyber security drills for B/Ds and stakeholders of Internet infrastructure.

[2] GovCERT.HK was set up under OGCIO in April 2015 to coordinate information and cyber security incidents. GovCERT.HK is the coordination centre for government IT administrators and users on computer emergency response and incident handling. It works closely with HKCERT on threats and incidents that would affect the private sectors and the community. Globally, GovCERT.HK would collaborate with other governmental and regional CERTs and international organizations with a view to facilitating exchange of information and knowledge needed to reduce vulnerabilities, mitigate risks, and react upon threats and attacks.

Information security initiatives in the wider community

Monitoring of cyber security of large-scale events

15. As regards the protection of Internet infrastructure, OGCIO activates the security alert mechanism of the Internet Infrastructure Liaison Group[3] ("IILG") as necessary to strengthen monitoring of cyber security of large-scale events and provide support events to protect the local Internet infrastructure against alleged cyber attacks.

Local collaboration

16. OGCIO provides funding support for HKCERT to coordinate computer security incident response, monitor and disseminate security alerts, promote information security awareness to local enterprises and the public.

International liaison

17. GovCERT.HK maintains close liaison with other regional CERTs through joining the CERT Coordination Centre, the Forum of Incident Response and Security Teams, and the Asia Pacific Emergency Response Team ("APCERT") to facilitate timely sharing of information on security threats, vulnerabilities and security incidents. The Government also actively participates in technological exchange activities held by the organizations, including the APCERT Drill. It also regularly participates in the meetings of the International Organization for Standardization on IT Security Techniques (ISO/IEC JTC1/SC27) to follow the latest developments in technologies and standards related to information security.

Supporting small and medium enterprises

18. OGCIO works with HKCERT and relevant organizations to arrange seminars for small and medium enterprises ("SMEs") to raise their awareness of cyber threats, and share with them the best practices to manage information security risks. Initiatives that the Administration has implemented include:

[3] OGCIO established IILG in 2005 to maintain close liaison with Internet infrastructure stakeholders and strive to sustain the healthy operation of the Internet infrastructure. IILG is chaired by the Deputy Government Chief Information Officer (Consulting and Operations) with members including representatives from OGCIO, HKCERT, HKPF, Hong Kong Internet Exchange, Hong Kong Internet Registration Corporation Limited, Hong Kong Internet Service Providers Association and Office of the Communications Authority.

(a) promoting, with HKCERT, the "Check-Act-Verify" approach to help SMEs identify potential cyber threats, take improvement measures and verify the effectiveness of the measures with a view to enhancing the overall cyber security level of SMEs;

(b) launching the "SME Free Web Security Health Check Pilot Scheme" jointly with various local trade associations, including The Chinese Manufacturers' Association of Hong Kong, the Federation of Hong Kong Industries, the Hong Kong General Chamber of Commerce, the Hong Kong Small and Medium Enterprises Association and the SME One of the Hong Kong Productivity Council to promote awareness of information security and cyber threats to SMEs and help them build a more secured e-business environment;

(c) launching various publicity and education activities, including thematic seminars, radio programmes, distribution of information leaflets, etc., to remind businesses to strengthen cyber security measures and protect their information systems as well as data assets; and

(d) organizing the "SME's Cloud Security Forum" in September 2016 through the collaboration of OGCIO and the Support and Consultation Centre for SMEs of the Trade and Industry Department where SMEs and security experts shared and discussed the security considerations for cloud service acquisition and adoption

19. GovCERT.HK has been collaborating closely with HKCERT and CERTs of other places to share information on cyber security threats and coordinate incident response, and helps provide early warnings to the public. In addition to sharing cyber security information, GovCERT.HK also participates in cooperative events with the CERT community including sharing of knowledge and skills, training and workshops and cross-border incident response drills of a regional and global nature.

Support to the public to tackle malware

20. OGCIO, HKPF and HKCERT have organized seminars with the theme of "Protecting Data from Ransomware Attacks" for critical infrastructure operators, businesses and organizations, schools and the general public to enhance their understanding of the infection paths, impacts and processes of ransomware. Strategies and techniques in addressing

ransomware attacks were covered. Information on ransomware attacks has been disseminated to SMEs and the general public through the Cyber Security Information Portal (www.cybersecurity.hk), newspapers and electronic media.

Public awareness and education

21. The Administration regularly arranges activities and awareness training for the public on the latest best practices to protect computing devices and information assets against cyber security risks. OGCIO would stage year-round activities with HKPF, HKCERT and other organizations to raise public awareness on information security. These activities include:

(a) organizing seminars and dissemination of the latest security alerts and information to the public through the Government websites as well as other media and publicity channels;

(b) conducting school visits, in collaboration with information security professional organizations, to educate local young people about the knowledge of information security and the proper attitude in using the Internet;

(c) holding the "Hong Kong – Mainland Cyber Security Forum 2016" where cyber security experts of Hong Kong and the Mainland shared their in-depth analysis on the cyber security challenges and associated technical solutions in the areas of financial technology, cloud computing, big data, etc.;

(d) organizing the "Cyber Security Professionals Awards" in September 2016. This event, which was co-organized by OGCIO, HKPF and HKCERT, encouraged personnel who had contributed to the information security industry to share and exchange their insights in order to enhance the industry's capabilities of cyber security protection;

(e) holding, on a regular basis, various cyber security promotion events, including the annual "Build a Secure Cyberspace 2016", to raise public awareness of cyber security and the trend of cyber-attacks, and to encourage participants to strengthen protection of personal and sensitive data; and

(f) enriching the contents on the OGCIO's thematic Cyber Security Information Portal by, for example, featuring public events on information security, expert advice, information security stories contributed by professional organizations, etc., so as to provide practical tips and suggest useful tools for the public to protect their computer equipment and websites.

Previous discussions

Panel on Information Technology and Broadcasting

22. At the Panel on Information Technology and Broadcasting ("the Panel") meeting held on 12 December 2016, the Administration briefed members on the latest progress and development of the Government's information security programmes.

Public education and awareness

23. Some members expressed concerns about the lack of public awareness of cyber security risks, and asked how the Administration would address the issue. The Administration advised that information on the latest cyber security threats, such as ransomware attacks, as well as relevant security tips had been disseminated to SMEs and the general public through the Cyber Security Information Portal (www.cybersecurity.hk), newspapers and electronic media. A learning module entitled "Protect Yourself against Ransomware" which introduces proper preventive and responsive measures against ransomware attacks, had been produced to remind the public to take necessary precautions.

Measures against malware and phishing websites

24. Members enquired about the Administration's measures to enhance information security awareness of the public on phishing websites and malware, and the mitigation measures taken or mechanisms to be implemented. The Administration advised that OGCIO worked closely with HKCERT and the industry to share information with the community on security threats and vulnerabilities through various channels, including websites, newspapers, electronic media, mobile applications, public events and thematic talks.

25. OGCIO provided practical tips and suggested useful tools for the public to protect their computer equipment and websites through the Cyber

Security Information Portal. The "Technology Voucher Programme" launched by the Innovation and Technology Commission enabled SMEs to adopt technological services and solutions, including IT to enhance cyber security.

26. Furthermore, OGCIO worked with the Hong Kong Internet Registration Corporation Limited (administrator of ".hk" Internet domain names) to promote the use of Domain Name System Security Extensions to improve the trustworthiness of ".hk" websites, and collaborated with the industry and different organizations to launch various publicity and education activities, including thematic seminars, radio programmes, distribution of information leaflets, etc., to remind businesses to strengthen cyber security measures and protect their information systems as well as data assets.

27. As regards mitigating measures against phishing websites, the Administration informed the Panel that HKPF's Cyber Security and Technology Crime Bureau had established procedures and mechanisms to combat cyber-crimes, including tackling local and overseas phishing websites.

Manpower and training

28. Some members expressed concerns about shortage of information and communications technology ("ICT") manpower and enquired about the measures to be taken by the Administration to enhance training for development of ICT manpower. Panel members suggested that the Administration should conduct relevant manpower surveys on ICT industries at appropriate stages to enable the Government to gain better understanding of the ICT manpower demand.

29. The Administration had informed the Panel that OGCIO had been liaising with local universities and tertiary institutions on providing relevant education programmes for students and ICT staff, and had engaged in discussions with the ICT industry on providing more internship to encourage students and graduates to choose ICT as their career.

30. As regards certification of information security professionals, OGCIO would co-ordinate with information security professional bodies with a view to providing more professional courses and recognition for the development of ICT manpower. OGCIO had also provided professional training and recognition to Government staff to certify their knowledge in information security.

Measures against cyber attack

31. Some members enquired about the measures taken by the Administration to tackle cyber attacks within the Government. The Administration explained that OGCIO performed regular malware scans and would continue to explore the latest technologies, such as big data analytics, to improve network monitoring and malware detection for making prompt response and strengthening precautionary measures. OGCIO also reminded users in all B/Ds to abide by the Government's information security policies and guidelines, and to take appropriate precautionary measures in handling their emails and protecting government systems and data assets.

Council meetings

32. Members, including Hon Charles MOK, Hon Martin LIAO, Dr Hon CHENG Chung-tai and Dr Hon Elizabeth QUAT has raised written questions related to information security at Council meetings. Members' questions are listed in **Appendix**.

Finance Committee

33. At the special meeting of the Finance Committee held on 3 April 2017, Hon Charles MOK enquired about the measures on promoting cyber and information security in 2017-2018. Dr Hon Elizabeth QUAT also enquired about the Administration's existing policies, measures, work units and facilities for safeguarding the information system security of the Government and the community. Hon James TO enquired about the measures implemented by the Government to strengthen the enforcement of information technology security code of practice, policy and guidelines. The Administration's replies are listed in **Appendix**.

Latest position

34. The Administration will brief the Panel on 12 February 2018 on the progress and development of the Government's information security programmes.

Relevant papers

35. A list of the relevant papers is set out in the **Appendix**.

Council Business Division 4
Legislative Council Secretariat
6 February 2018

Appendix

List of relevant papers

Issued by	Meeting date/ Issue date	Paper
Council meeting	7 December 2016	Question No. 8 raised by Hon Martin LIAO Cyber security
	14 December 2016	Question No. 19 raised by Hon Charles MOK Information security in Hong Kong
	11 January 2017	Question No. 8 raised by Dr Hon CHENG Chung-tai CyberSecurity Information Sharing Platform and Cyber Intelligence Sharing Platform
	31 May 2017	Question No. 9 raised by Hon Charles MOK Information security of government departments, public bodies and organisations involved in public works projects
	7 June 2017	Question No. 22 raised by Dr Hon Elizabeth QUAT Capability of institutions in Hong Kong in coping with major computer security incidents
	29 November 2017	Question No. 15 raised by Hon Charles MOK Measures to enhance information security

Issued by	Meeting date/ Issue date	Paper
Panel on Information Technology and Broadcasting	12 December 2016	Administration's paper on update on information security LC Paper No. CB(4)246/16-17(04) Updated background brief on information security LC Paper No. CB(4)246/16-17(05) Minutes of meeting LC Paper No. CB(4)515/16-17
Special Finance Committee	3 April 2017	Administration's replies to Members initial written questions (Reply Serial Nos. ITB175, ITB203 and ITB207) http://www.legco.gov.hk/yr16-17/english/fc/fc/w_q/itb-e.pdf