立法會
Legislative Council

LC Paper No. CB(1)564/18-19(04)

Ref. : CB1/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 18 February 2019

Updated background brief on information security

Purpose

This paper provides background information on the Administration's information security programmes. It also summarizes the views and concerns expressed by Members in previous discussions on the subject.

Background

2. The objectives of the Administration's information security programmes are to:

(a) formulate and implement information security policies and guidelines for compliance and reference by bureaux and departments ("B/Ds");

(b) ensure that all the Administration's information technology ("IT") infrastructure, systems and information are secure and resilient; and

(c) 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 under the following three main areas:

(a) information security in the Government;
(b) information security initiatives in the community; and
(c) professional training and public awareness.

Information security in the Government

4. The Administration has implemented multiple layers of security measures to protect its information infrastructure and data assets against the increasing incidents of cyber attacks and related security threats within the Government. The relevant preventive measures implemented by the Administration include:

(a) *Monitoring cyber risk trends*: 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 to strengthen their precautionary measures;

(b) *Conducting risk assessment and follow-up*: B/Ds have implemented security-related measures, including conducting security risk assessments and audits, implementation of technical security solutions and upgrading of security infrastructure;

(c) *Data protection measures*: to ensure protection of government data assets, the Administration uses encryption of 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; and

(d) *Ransomware and malware attacks*: OGCIO issues high-risk security alerts and security reminders to B/Ds, including 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.

5. In addition, the Administration has formulated the "Government IT Security Policy and Guidelines" to strengthen B/Ds' compliance requirements and security practices to cope with different types of emerging threats. As regards staff training efforts, the Administration has been arranging training for support personnel to update their knowledge on emerging threats and technical skills to mitigate risks. 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.

Information security initiatives in the community

Local collaboration

6. OGCIO provides funding support for the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") to coordinate computer security incident responses, monitor and disseminate security alerts, as well as promote information security awareness to local enterprises and the public. HKCERT also collaborates with Internet services providers to promote information security best practices in order to make Hong Kong a safe Internet hub.

International and regional cooperation

7. The Government Computer Emergency Response Team Hong Kong ("GovCERT")[1] maintains close liaison with other regional CERTs through the CERT Coordination Centre, the Forum of Incident Response and Security Teams ("FIRST"), and the Asia Pacific Computer Emergency Response Team ("APCERT") to facilitate timely sharing of information on security threats, vulnerabilities and security incidents. To foster collaborative exchanges and sharing of information security intelligence, GovCERT actively participates in relevant activities organized by different organizations, including the joint annual incident response drill organized by APCERT.

Support for small and medium enterprises

8. To strengthen the long-term competitiveness of small and medium enterprises ("SMEs"), the Government has launched the $500 million Technology Voucher Programme ("TVP") under the Innovation and Technology Fund on a pilot basis in November 2016 to subsidize SMEs in using technology services and solutions to improve productivity or upgrade and transform their business processes. Subsidies under TVP can also be used on the adoption of cyber security solutions that provide SMEs with the

[1] GovCERT was set up under OGCIO in April 2015 to coordinate information and cyber security incidents. GovCERT 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 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.

means to defend against cyber attacks and disaster recovery solutions.

Professional training and public awareness

9. As regards vocational training, the Hong Kong Productivity Council, HKCERT and GovCERT, together with other organizations from time to time, organize conferences, thematic seminars and workshops, including certificate courses on information security and the annual "Information Security Summit" to enhance IT practitioners' skills and knowledge of information security. Meanwhile, OGCIO, the Hong Kong Police Force ("HKPF") and HKCERT have organized cyber security seminars to help enterprises, schools and the public understand the risks associated with Internet-connected devices, and remind them to stay vigilant to guard against security vulnerabilities as well as take appropriate security measures to ensure the safety of these devices and data.

Previous discussions

Panel on Information Technology and Broadcasting

10. The Administration briefed the Panel on Information Technology and Broadcasting ("the Panel") on 12 February 2018 on the latest development of the Government's information security programmes.

Information and cyber security landscape

11. Members queried the reasons for the decrease in the number of computer security incidents handled by HKCERT. The Administration attributed the decrease (except malicious software and botnet incidents) to promotion and publicity efforts implemented by the Administration and HKCERT which had enhanced users' awareness in computer security and led to their adoption of preventive measures.

12. Some members asked about the investigation of the lost of two government computers, which stored personal information of more than three million voters, during the last Legislative Council elections in 2016. The Administration advised that, following the incident, OGCIO had provided advice and reminded the Registration and Electoral Office on the need to comply with the various information security guidelines. The Administration indicated that there was no evidence of personal information leakage.

Support for small and medium enterprises

13. Despite the availability of subsidy under TVP, some members pointed

out that many SMEs were wary of the potential high cost of computer security systems and were reluctant to invest in hardware and software solutions against cyber attacks. Members queried whether the subsidies provided under TVP was sufficient. Some members suggested that the Administration should provide information about less costly options such as services offered by the Hong Kong Productivity Council which helped SMEs evaluate the risks of their current systems and recommended improvement measures before SMEs spent any money on information security solutions.

14. The Administration responded that successful applicants could spend up to $300,000, which should normally be sufficient for purchasing technology services and solutions to improve security of their information systems. The Administration would step up promotion and encourage SMEs to make applications under TVP to improve security of their information systems.

Review of legislation for protection of personal information

15. Some members enquired whether the Administration had identified any legal provisions that should be brought up-to-date to enhance protection of individuals, especially children and their personal data in the light of the increasing prevalence of online activities such as Internet payment and other online commercial activities. Members also asked if OGCIO would play a more proactive role in initiating legislative reviews and providing guidelines to the relevant B/Ds.

16. The Administration advised that OGCIO would update internal guidelines and policies on a regular basis to strengthen information security protection. Other B/Ds, as well as the respective statutory organizations, would also keep the respective legislation and guidelines under review. The Administration has subsequently provided a plan for legislative review in view of the privacy and information security issues arising from the development of e-commerce, Internet of things, financial technology, etc. which is provided through a hyperlink in the **Appendix**.

Helping victims of cyber crime to recover lost data

17. Some members asked if HKPF would help victims of cyber crime and Internet fraudulent cases to recover their data and reduce loss. The Administration advised that HKPF had advised owners of websites to take precautions and remove malware from their systems, and would alert smartphone owners to clear malware from their devices. Furthermore, the Administration would set up a cross-sector platform for sharing information and analyses on the various cyber security risks and vulnerabilities, and would disseminate the information to the community. However, the

Administration explained that it was difficult for the Police or any organization or individual to recover data encrypted by ransomware.

International and regional collaboration

18. Members expressed concerns on whether GovCERT's participation in international conferences was cost-effective. The Administration responded that participation in annual conferences, such as those organized by FIRST and APCERT, had been effective in enabling GovCERT to establish a communication network with regional and international organizations for information exchange. This would enable the Administration to collect latest information on security risks, for example, attacks by latest malware and ransomware, and offer advice to the general public.

Professional training and public awareness

19. Some members suggested that the Administration should introduce more training programmes that enabled trainees to be awarded internationally accredited qualifications in information security. They also asked if the Administration would provide subsidies for SMEs to support their employees to undergo such training.

20. The Administration indicated that it had been collaborating with relevant professional bodies to encourage IT personnel to sit for professional examinations and obtain accredited qualifications. According to ISACA[2] and the International Information System Security Certification Consortium, about 4 500 qualifications in Certified Information Security Manager, Certified Information Security Auditor and Certified Information System Security Professional were being held by IT professionals in 2017, accounting for about 3% to 5% of all IT professionals in Hong Kong. The IT professionals with these relevant qualifications were capable of performing information security work.

21. Members had also expressed concerns about young people's awareness of cyber security in using mobile devices, cloud services and social media. The Administration explained that OGCIO and HKPF had organized various competitions for young people on cyber security-related matters, and would continue to conduct school visits in collaboration with information security professional associations.

[2] ISACA is formerly known as Information Systems Audit and Control Association and now goes by its acronym only.

Council meetings

22. Members, including Hon Martin LIAO, Hon Charles Peter MOK, Dr Hon CHENG Chung-tai, Dr Hon Elizabeth QUAT, Hon CHAN Hak-kan, Hon Tony TSE, Hon Paul TSE and Hon Alvin YEUNG, have raised questions related to information security at Council meetings. Details of the questions and the Administration's replies are given in the hyperlinks in the **Appendix**.

Special Finance Committee meetings

23. At the special meeting of the Finance Committee on 19 April 2018, members expressed concerns that hacker attacks on some local online service suppliers had led to the leakage of a lot of customer information. Members enquired about the Administration's measures to strengthen cyber security and its support to SMEs with a view to enhancing information security and protection.

Latest position

24. The Administration will brief the Panel on 18 February 2019 on the progress of the Government's information security programmes.

Relevant papers

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

Council Business Division 1
Legislative Council Secretariat
12 February 2019

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
	17 January 2018	Question No. 22 raised by Hon CHAN Hak-kan Privacy concerns brought about by smart products

Issued by	Meeting date/ Issue date	Paper
Council meeting	25 April 2018	Question No. 2 raised by Hon Tony TSE Police committed to combating technology crimes
	14 November 2018	Question No. 2 raised by Hon Charles MOK Enhancing information security and the protection for privacy of personal data
	12 December 2018	Question No. 5 raised by Hon Paul TSE Leakage of personal data by commercial organisations
	16 January 2019	Question No. 8 raised by Hon Alvin YEUNG Information security of using certain Chinese telecommunications products
Panel on Information Technology and Broadcasting	12 February 2018	Administration's paper on update on information security (LC Paper No. CB(4)577/17-18(03)) Updated background brief on information security (LC Paper No. CB(4)577/17-18(04)) Administration's response to issues raised at the meeting on 12 February 2018 (LC Paper No. CB(4)1522/17-18(01)) Minutes of meeting (LC Paper No. CB(4)832/17-18)

Issued by	Meeting date/ Issue date	Paper
Special Finance Committee	19 April 2018	Administration's replies to Members initial written questions (Reply Serial Nos. ITB203, ITB204, ITB212, ITB225, ITB241 and ITB244) Minutes of meeting