立法會
Legislative Council

LC Paper No. CB(1)306/19-20(06)

Ref.: CB1/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 13 January 2020

Updated background brief on information security

Purpose

This paper provides background information on the Administration's information security programmes. It also summarizes the major 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 Government;

(b) information security initiatives in the community; and

(c) professional training and public awareness.

Information security in 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 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*: B/Ds have implemented security-related measures, including conducting security risk assessments and audits;

(c) *Security technology measures*: the Administration has implemented security measures, including firewalls, anti-distributed denial-of-service solutions, intrusion detection and prevention systems, data encryption, anti-virus solutions, real-time monitoring tools, etc.; and

(d) *Security alerts*: the Administration has implemented a cyber-threat information sharing platform within Government to strengthen monitoring of cyber security threats and sharing of relevant information. Security alerts related to computer systems or software vulnerabilities are issued through this platform to remind B/Ds to take early and appropriate preventive measures.

5. In addition, the Administration has formulated the "Government IT Security Policy and Guidelines" ("Policy and Guidelines") to strengthen B/Ds' compliance requirements and security practices to cope with different types of emerging threats. Information security compliance audits are conducted to ensure B/Ds' compliance with the Policy and Guidelines and

recommendations for improvements are made to them. The Administration has indicated that a review of the Policy and Guidelines would be conducted in 2019.

6. As regards staff training, the Administration has organized seminars and solution showcases, for departmental management personnel and information security staff. These training activities covered the latest cyber security trends such as security knowledge related to Internet of Things, smart city, phishing, etc.

Information security initiatives in the community

Local collaboration

7. OGCIO provides funding support for the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT")[1] 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

8. The Government Computer Emergency Response Team Hong Kong ("GovCERT")[2] maintains close liaison with other regional CERTs through the CERT Coordination Centre, the Forum of Incident Response and Security Teams, and the Asia Pacific Computer Emergency Response Team

---

[1] The Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") was established by the Government in 2001 and managed by the Hong Kong Productivity Council to provide local enterprises and Internet users with services related to computer security incidents. These include collecting intelligence on information security threats and publishing latest information to enhance the public's security awareness, as well as providing advice on suggested measures to take in response to important security threats such as phishing attacks and ransomwares.

[2] The Government Computer Emergency Response Team Hong Kong ("GovCERT") was set up under the Office of the Government Chief Information Officer in April 2015 to coordinate information and cyber security incidents. GovCERT is the coordination centre for government information technology 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 Computer Emergency Response Teams 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.

("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

9. The Innovation and Technology Commission expanded the scope of funding support and increased the level of subsidy under the Technology Voucher Programme ("TVP")[3] in February 2018. All local non-listed companies, including small and medium enterprises ("SMEs"), can apply for subsidies to procure services and solutions to guard against cyber-attacks and perform disaster recovery so as to further reduce information security risks. To assist SMEs to cope with potential information security risks, HKCERT and OGCIO have collaborated with industry associations to organize relevant conferences, thematic seminars and workshops covering topics such as applications of cloud computing and artificial intelligence.

Pilot Partnership Programme for Cyber Security Information Sharing

10. OGCIO launched a two-year Pilot Partnership Programme for Cyber Security Information Sharing ("Pilot Partnership Programme") in September 2018 and took the lead to set up a cross-sector Cyber Security Information Sharing and Collaborative Platform (Cybersechub.hk). Through the platform, members of the Pilot Partnership Programme can exchange information on cyber security threats, mitigation solutions, best practices, etc. and disseminate relevant information to the public in a timely manner.

Public awareness

11. In view of the latest incidents and trends of phishing attacks including fraudulent websites and phishing emails, OGCIO, Hong Kong Police Force ("HKPF") and HKCERT have organized a series of promotional activities to raise public awareness against cyber frauds. OGCIO has also set up a one-stop thematic web page "Beware of Phishing Attacks" under the Cyber Security Information Portal. Other information security messages are also disseminated to the public through the Cyber Security Information Portal and various promotional channels. HKPF has launched cyber security campaigns to raise public awareness in protection of mobile smart devices, and provide

[3] The Government launched the $500 million Technology Voucher Programme under the Innovation and Technology Fund on a pilot basis in November 2016 to subsidize small and medium enterprises in using technology services and solutions to improve productivity or upgrade and transform their business processes.

free-of-charge mobile anti-virus and scanning software to help protect their devices against cyber-attacks including botnet and malicious software. Furthermore, OGCIO has collaborated with professional bodies in organizing school visits to enhance the knowledge of information security and promote the correct attitude towards the use of the Internet for teachers and students.

Professional training

12. The Administration collaborates with the industry to organize conferences, thematic seminars and workshops, including the annual "Information Security Summit", to encourage and support the industry in information security training. The Administration also works with professional bodies to promote professional accreditation in information security among IT practitioners for enhancing their knowledge and skills in information security, and encourages them to join the information security profession with a view to nurturing more qualified professionals. In addition, the Administration actively encourages tertiary education institutions to provide more information security courses in relevant disciplines to train up more talents with information security expertise and skills.

Previous discussions

Panel on Information Technology and Broadcasting

13. The Administration briefed the Panel on Information Technology and Broadcasting ("the Panel") on 18 February 2019 on the latest overall situation of information security in Hong Kong and the Government's work in information security. The major views and concerns expressed by members are summarized in the ensuing paragraphs.

Measures to strengthen information security management of enterprises

14. In light of the rising trend in information security incidents and technology crimes in Hong Kong, members asked what public education and publicity measures the Administration would implement to raise the awareness of local enterprises on information security, and whether resources support would be provided for local SMEs to improve their security systems.

15. The Administration advised that OGCIO had launched a local cross-sector platform (Cybersechub.hk) (paragraph 10) under the Pilot Partnership Programme to enhance Hong Kong's overall defence and resilience against cyber-attacks. The Innovation and Technology Bureau would explore measures to enhance technical support, such as website vulnerability

scanning, for local organizations including SMEs with websites registered under the ".hk" domain. Apart from engaging HKCERT to publish useful guidelines for SMEs, etc., OGCIO would also disseminate information on handling security issues such as email frauds, malware, etc., through social and electronic media, and promote best security practices.

Measures to tackle cyber security threats in Government

16. In tackling cyber security threats in government systems, members asked whether the Administration would engage hackers to test the robustness of their systems. The Administration informed members that rounds of ethical hacking were conducted on its systems, and the security risks were being assessed on a regular basis. Multiple layers of security measures, including firewalls, intrusion detection and prevention systems, had been implemented.

Support for the technology sector and local enterprises

17. Members had exchanged views with the Administration on the scope and objectives of the Pilot Partnership Programme and the support under TVP. The Administration highlighted that through Cybersechub.hk, participants could share information on cyber security threats, mitigation solutions, best practices, etc. SMEs could use the financial support to procure technology services and solutions to improve productivity, upgrade or transform business processes and enhance information security.

Other measures to promote information security

18. Members asked how the Administration would nurture information security talent in Hong Kong. The Administration responded that it had included experienced cyber security specialists in the first Talent List of Hong Kong[4], and had encouraged tertiary education institutions to offer more information security training courses in relevant disciplines to nurture more talents.

Measures to regulate online privacy and related issues

19. Members commented that the Administration should consider introducing legislation to regulate online privacy and related issues. They suggested that the Administration might draw reference from General Data

[4] The Talent List of Hong Kong is drawn by the Government to attract high quality talents in an effective and focused manner to support Hong Kong's diversified economy. The List comprises 11 professions. Talents under the List are eligible for the immigration facilitation under the Quality Migrant Admission Scheme.

Protection Regulation adopted by the European Union, which included new provisions requiring data processors or controllers to implement technical measures to ensure compliance with overseas data protection regimes.

20. The Administration advised that a subcommittee under the Law Reform Commission of Hong Kong had commenced a study on cybercrime in January 2019. The Constitutional and Mainland Affairs Bureau, in collaboration with the Privacy Commissioner for Personal Data, was reviewing the relevant provisions and penalties under the Personal Data (Privacy) Ordinance (Cap. 486), and would consider how the regulatory framework could be enhanced, in particular with respect to data breach notification.

Incident of personal data leakage

21. On 24 October 2018, Cathay Pacific Airways Limited ("Cathay Pacific") announced an incident of leakage of passengers' personal data affecting approximately 9.4 million passengers globally. The Panel, Panel on Constitutional Affairs and Panel on Security held a joint meeting on 14 November 2018 to discuss the incident.

22. Members were concerned that Cathay Pacific informed the Police and the public only months after it had discovered the breach. Cathay Pacific explained that it had taken quite some time in conducting scenario assessment, containment and remediation according to the company's internal procedure before contacting its passengers about the types of personal data that might have been affected.

23. Members held the view that the existing level of penalty in Cap. 486 should be increased to deter delay in the disclosure of data breaches. The Administration explained that a review of Cap. 486 would be conducted shortly, and introduction of a mandatory requirement for notification, the prosecution process in respect of breach of such requirement as well as the penalty level would be among the areas to be considered.

24. Some members demanded Cathay Pacific to compensate affected passengers financially, restore the company's goodwill and/or dissolve the management board to demonstrate accountability. Cathay Pacific responded that affected customers could claim compensation from the company for any direct financial losses.

Finance Committee

25. At the special meeting of the Finance Committee to examine the

Estimates of Expenditure 2018-2019 and 2019-2020 held on 19 April 2018 and 11 April 2019 respectively, members expressed concerns that hacker attacks on some local online service suppliers had led to the leakage of a lot of customer information. Members also enquired about the Administration's measures to strengthen cyber security and its support to SMEs with a view to enhancing information security and protection.

Questions raised at Council meetings

26. Members, including Hon Charles Peter MOK, Hon Paul TSE, Hon Alvin YEUNG and Hon Jimmy Ng, 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**.

Latest position

27. The Administration will brief the Panel on 13 January 2020 on the development of the Government's information security programmes.

Relevant papers

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

Council Business Division 1
Legislative Council Secretariat
7 January 2020

Appendix

List of relevant papers

Meeting	Date of meeting	Papers
Panel on Information Technology and Broadcasting, Panel on Constitutional Affairs and Panel on Security	24 October 2018	Administration's paper on the incident of leakage of passengers' personal data by Cathay Pacific Airways and issues relating to protection of personal data and cyber security (LC Paper No. CB(2)222/18-19(01)) Paper provided by Cathay Pacific Airways (LC Paper No. CB(2)222/18-19(02)) Background brief on issues relating to protection of personal data and cyber security (LC Paper No. CB(2)222/18-19(03)) Minutes of meeting (LC Paper No. CB(1)1329/18-19)
Panel on Information Technology and Broadcasting	18 February 2019	Administration's paper on update on information security (LC Paper No. CB(1)564/18-19(03)) Updated background brief on information security (LC Paper No. CB(1)564/18-19(04)) Administration's response to issues raised at the meeting on 18 February 2019 (LC Paper No. CB(1)735/18-19(01)) Minutes of meeting (LC Paper No. CB(1)838/18-19)

Meeting	Date of meeting	Papers
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
	11 April 2019	Administration's replies to Members initial written questions (Reply Serial Nos. ITB209 and ITB216) Minutes of meeting
Council meeting	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
	22 May 2019	Question No. 11 raised by Hon Jimmy Ng Security issues of the use of QR codes