立法會
Legislative Council

LC Paper No. CB(1)868/20-21(05)

Ref.: CB1/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 10 May 2021

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. To protect the government's information infrastructure and data assets against the increasing incidents of cyber-attacks and related security threats, the Office of the Government Chief Information Officer ("OGCIO") has implemented relevant preventive measures including monitoring cyber risk trends, conducting independent compliance audits of B/Ds and providing technical support to B/Ds. 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.

5. As regards staff training, the Administration has organized seminars and solution showcases to enhance the knowledge of information security among government staff. OGCIO also encourages its staff to obtain internationally recognized information security certificates to strengthen their expertise in information security.

Information security initiatives in the community

Local collaboration

6. 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 cooperation

7. The Government Computer Emergency Response Team Hong Kong

[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.

("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 ("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.

Enhancing the capability of Hong Kong enterprises (including small and medium enterprises) in responding to various cyber attacks

8. The Government launched the Technology Voucher Programme in 2016 to encourage more local enterprises, including small and medium enterprises ("SMEs"), to make use of technology, including enhancement of cyber security measures to deal with cyber threats.

9. The Government also joined hands with the Hong Kong Internet Registration Corporation Limited ("HKIRC") to launch a free SME website scanning service to assist SMEs in identifying potential security vulnerabilities as early as possible. Given the importance of cyber security to individual sectors, HKCERT continues to join hands with relevant industry associations to organize thematic seminars to further promote cyber security awareness of practitioners from various sectors, including financial services, healthcare, retail and trade, property management, hotels and tourism, manufacturing, education, IT, etc.

Cyber Security Information Sharing and Collaborative Platform

10. To promote the sharing of cyber risk information among industries and enterprises, OGCIO launched the "Pilot Partnership Programme for Cyber Security Information Sharing" in 2018 and took the lead to set up a cross-sector "Cyber Security Information Sharing and Collaborative Platform" (Cybersechub.hk). The platform enables the industries and enterprises to share information on cyber security threats, mitigation

---

[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.

measures and best practices. It also provides an open section for the public to obtain security alerts and advice provided by experts.

Public awareness

11. In relation to the threat from phishing, OGCIO, the Hong Kong Police Force ("Police Force") and HKCERT conducted in 2019 a series of promotional activities under the theme "We Together! Secure Data!" to promote public awareness of information security, especially data protection. OGCIO has also disseminated different forms of cyber security information to the public through various channels and organized school visits with professional bodies to convey messages about information security. The Police Force has organized the "Cyber's Got Talent Carnival" to educate the school community on the importance of cyber security for computers and mobile devices.

Manpower resources in information security

12. The Administration announced in 2019 its decision to enhance the Technology Talent Admission Scheme [3] by expanding the scope of the scheme to research and development companies outside the Hong Kong Science & Technology Parks and Cyberport to allow more local technology companies to recruit technology talent from overseas and the Mainland to meet the demand of specific technology areas including cyber security. In addition, the Administration encourages local tertiary education institutions to introduce information security courses under different disciplines in order to sustain a stable supply of information security talent. In the area of professional training, the Administration works with information security professional bodies to promote professional accreditation in order to nurture more IT practitioners with professional knowledge and skills in information security.

Previous discussions

13. The Administration briefed the Panel on Information Technology and Broadcasting ("the Panel") on 13 January 2020 on the overview of information and cyber security situation in Hong Kong. Related issues were brought up during examination of the Estimates of Expenditure in April 2020. Members' major views and concerns are summarized in the ensuing paragraphs.

---

[3] The Technology Talent Admission Scheme was launched in 2018 to provide a fast-track arrangement to admit overseas and Mainland technology talent to undertake research and development work.

Overall situation of information and cyber security

14. Members expressed concerns about the total financial losses that might be attributed to technology crimes, and enquired about the preventive measures. In particular, measures to combat cross-boundary technology crimes, and strengthen cooperation with overseas stakeholders and law enforcement agencies to counter prevalent technology crimes and cyber threats.

15. The Administration advised that OGCIO was working closely with HKCERT and the Police Force to promote public awareness of information security, through disseminating security-related information and providing advice on preventive measures against security threats. Meanwhile, the Police Force exchanged intelligence with various law enforcement agencies to keep track of the crime trends and study ways to combat cross-boundary criminal activities. HKIRC had also launched a new and free website scanning service to assist SMEs in identifying potential security vulnerabilities.

16. Members noted that many teachers and students of universities, primary and secondary schools were using web conferencing software Zoom for online classes while government organizations in many regions (such as the Ministry of Defence of the United Kingdom) had forbidden their staff from using Zoom. Members enquired about the Administration's work on information security, including whether it would issue safety tips on the use of Zoom to the public (universities, primary and secondary schools particularly). Members also asked the Administration to step up promotion and public education on cyber security.

17. The Administration advised that the Education Bureau had issued the "Reference principles on supporting students' home learning with e-learning modes during class suspension" to local public primary and secondary schools for their reference. In addition, HKCERT had issued advice to the public on security measures to protect the meetings in Zoom, including suggesting that users should not share confidential information during the meetings, be vigilant about suspicious activities of their accounts, and Zoom meeting hosts should exercise care in handling meeting records to ensure safety and protect the privacy of meeting participants, etc.

Measures to tackle cyber security threats in Government

18. Noting that OGCIO had an established mechanism to assist B/Ds in conducting webpage scanning and penetration testing, some Panel members sought information about the government departments that were more

vulnerable to cyber-attacks and the major types of government services that received the heaviest attacks. Some Panel members asked if the Administration had anticipated any different emerging cyber threats arising from the increasing adoption of cloud computing services by government departments, and how B/Ds would manage those risks. To cope with the rapid technological development such as 5G and Internet of Things, Panel members were concerned about how the Administration would prepare B/Ds and help the industry to be prepared to tackle any new risks involved. Members also took the view that the Administration should actively share relevant cyber threat intelligence with large enterprises as well as SMEs, as such information would provide useful pointers for local companies to strengthen their precautionary measures.

19. Some Panel members queried whether the Police Force had bought hacking software which allowed them to unlock smartphones and access user data without the owners' consent, and adopted facial recognition technology to identify suspects in the course of criminal investigations. Members also queried whether B/Ds, including the Police Force, had consulted OGCIO prior to their procurement of IT security software. The Administration advised that B/Ds would, according to their needs, implement security technology measures and procure IT security software. While there was no need for B/Ds, including the Police Force, to consult OGCIO's views prior to their procurement of relevant equipment and software, B/Ds should ensure that the procurement would comply with relevant laws and regulations.

20. Members enquired how OGCIO could ensure that all B/Ds would comply with the security requirements of the Government. The Administration advised that B/Ds were required to conduct information security risk assessments and audits once every two years to ensure that they had adopted effective security measures. OGCIO would also conduct independent information security compliance audits for all B/Ds every two years to assist them in continuously improving their security management systems to tackle emerging security threats.

Measures to strengthen information security management of enterprises

21. Members urged the Administration to step up efforts, in conjunction with industry associations, to promote the awareness of large enterprises and SMEs on system security risks. Members also suggested that the Administration should consider enhancing support for SMEs to cope with potential information security risks. The Administration advised that HKCERT would continue to collaborate with the industry associations and HKIRC to organize thematic seminars with a view to further promoting cyber security awareness.

Protection of privacy

22. Citing the incident where the Registration and Electoral Office lost two notebook computers containing voters' information, some Panel members queried whether the Administration would identify technology solutions to improve the protection of personal privacy and data. The Administration advised that efforts would continue to promote the awareness and knowledge of cyber security threats, preventive measures and best practices among the industries and in the community through education programmes, publicity programmes on radio, etc.

Law reform proposals under consideration or in the process of being implemented

23. In the course of discussion with the Administration on legislative measures to combat cybercrimes, Panel members noted that the Administration would consider introducing relevant legislation, such as provisions against voyeurism, reviewing "access to computer with criminal or dishonest intent" under section 161 of the Crimes Ordinance (Cap. 200), reviewing existing legislation on cybercrime, etc. Members urged the Administration to commence the relevant legislative process as early as practicable.

Recent development

24. On combating voyeurism, the Administration has introduced the Crimes (Amendment) Bill 2021 to the Legislative Council on 24 March 2021. The Bill provides for new offences on voyeurism, non-consensual recording of intimate parts, publication of images originating from voyeurism or non-consensual recording of intimate parts, publication or threatened publication of intimate images without consent and related matters.

Questions raised at Council meetings

25. Members had raised questions related to information security and protection of online privacy at various Council meetings. The questions and the Administration's written replies are provided in hyperlinks in the **Appendix**.

Latest position

26. The Administration will brief the Panel on 10 May 2021 on the progress and development of the Government's information security

programmes.

Relevant papers

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

Council Business Division 1
Legislative Council Secretariat
4 May 2021

Appendix

List of relevant papers

Meeting	Date of meeting	Papers
Meeting of the Panel on Information Technology and Broadcasting	13 January 2020	Administration's paper on update on information security (LC Paper No. CB(1)306/19-20(05)) Updated background brief on information security (LC Paper No. CB(1)306/19-20(06)) Administration's response to issues raised at the meeting on 13 January 2020 (LC Paper No. CB(1)479/19-20(01)) Minutes of meeting (LC Paper No. CB(1)480/19-20)
Special meeting of the Finance Committee for examination of Estimates of Expenditure 2020-2021	8 April 2020	Written questions raised by Members and the Administration's replies (Reply Serial Nos. ITB153 and ITB192) Report on the examination of the Estimates of Expenditure 2020-2021
Council meeting	22 April 2020	Question No. 7 raised by Hon Yung Hoi-yan Information security measures of the Government
	27 January 2021	Question No. 18 raised by Hon Elizabeth QUAT Protection of online privacy