立法會

Legislative Council

LC Paper No. CB(2)222 /18-19(03)

Ref : CB2/PL/CA+ CB4/PL/ITB+ CB2/PL/SE

Panel on Constitutional Affairs, Panel on Information Technology and Broadcasting and Panel on Security

Background brief prepared by the Legislative Council Secretariat for the joint meeting on 14 November 2018

Issues relating to protection of personal data and cyber security

Purpose

This paper summarizes the past discussion of the Panel on Constitutional Affairs ("CA Panel"), the Panel on Information Technology and Broadcasting ("ITB Panel") and the Panel on Security on issues relating to the protection of personal data and cyber security.

Background

Protection of Personal Data

2. The Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486), having come into force since 1996, aims to protect the individual's right to privacy with respect to personal data. PDPO applies to any data relating directly or indirectly to an individual, from which it is practicable to ascertain the identity of the individual and which is in a form in which access to or processing is practicable. Users of personal data in both public and private sectors are subject to the provisions of PDPO.

3. The Administration conducted a comprehensive review of PDPO with the support of the Privacy Commissioner for Personal Data ("PCPD"), and consulted the public from August to November 2009 on proposals arising from the review. The Administration published the consultation report in October 2010 [LC Paper No. CB(2) 37/10-11(02)] and further consulted the public on the legislative proposals from October to December 2010. The Report on Further Public Discussions on Review of PDPO was published in April 2011. The Ordinance

was amended in mid-2012 and all the amended provisions have already come into operation.[1]

4. The main features of PDPO are as follows:

(a) it establishes PCPD, which is an independent statutory authority, to promote and enforce compliance with PDPO;

(b) it gives statutory effect to internationally-accepted data protection principles, which provide for the fair collection of personal data; accuracy of personal data; duration for retention of personal data; limits on the use of personal data; security of personal data; openness by data users about the kinds of personal data they hold and purposes to which they are put; as well as data subjects' rights of access and correction with respect to their personal data;

(c) it regulates the use of personal data in direct marketing and the provision of personal data for use in direct marketing;

(d) it provides for offences against the disclosure of personal data obtained without consent from data users;

(e) it gives PCPD powers to approve and issue codes of practice giving guidance on compliance with PDPO; inspect personal data systems and investigate suspected breaches of the requirements under PDPO;

(f) it subjects the automated comparison of personal data to suitable control to protect the privacy interests of data subjects;

(g) it provides for a broad exemption for personal data held for domestic purposes and narrowly defined exemptions from the requirements on subject access and use limitation to cater for a variety of competing public and social interests, such as human resources management; security, defence and international relations;

[1] The Personal Data (Privacy) (Amendment) Ordinance 2012 ("Amendment Ordinance") was passed by the Legislative Council on 27 June 2012. The Amendment Ordinance introduced amendments to PDPO, inter alia, to provide for regulation over the use of personal data in direct marketing and provision of personal data for use in direct marketing; to create a new offence for disclosure of personal data obtained without consent from data users; to empower PCPD to provide legal assistance to aggrieved data subjects in bringing proceedings to seek compensation from data users under PDPO; to impose a heavier penalty for repeated contravention of enforcement notices; and to create a new offence for repeated contravention of the requirements under PDPO for which enforcement notices have been served.

the prevention and detection of crime; the assessment or collection of taxes; financial regulation; an individual's physical or mental health; news gathering and reporting, legal proceedings, due diligence exercise, and emergency situations; and

(h) it gives PCPD power to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user.

Cyber security

5. According to the Administration, the Government attaches great importance to information security and cyber security. The Office of the Government Chief Information Officer ("OGCIO") and its Government Computer Emergency Response Team ("GovCERT") have been closely monitoring the overall cyber security situation in Hong Kong. In collaboration with the Cyber Security and Technology Crime Bureau ("CSTCB") under the Hong Kong Police Force and the Hong Kong Computer Emergency Response Team Coordination Centre under the Hong Kong Productivity Council, OGCIO and its GovCERT have also been providing different stakeholders with support in relation to cyber security.

Discussion of relevant Panels

Enforcement power of the Privacy Commissioner for Personal Data

6. During discussion of review of PDPO by the CA Panel, members had expressed diverse views on PCPD's proposals of granting criminal investigation and prosecution power to PCPD, empowering PCPD to award compensation to aggrieved data subjects, and requiring a data user to pay monetary penalty for serious contravention of Data Protection Principles ("DPPs")[2] of PDPO. Nevertheless, members in general expressed concern that PCPD had inadequate powers for the effective enforcement of PDPO.

[2] Data users must follow the fair information practices stipulated in the six DPPs in Schedule 1 to PDPO in relation to the purpose and manner of data collection, accuracy and duration of data retention, use of personal data, security of personal data, availability of data information, and access to personal data. PCPD is empowered to direct the data user concerned to take corrective actions for non-compliance with the provisions of DPPs by issuing an enforcement notice. With effect from 1 October 2012, if a data user fails to take corrective actions for his contravention by the date specified in an enforcement notice, he will be liable to a fine at level five (at present $50,000) and imprisonment for two years. The data user is liable to a daily penalty of $1,000 if the offence continues. On a second or subsequent conviction, the maximum penalty is a fine at level six (at present $100,000) and imprisonment for two years.

7. At the CA Panel meetings on 15 and 20 November 2010, the former PCPD pointed out that the recent serious contraventions of PDPO and unauthorized sale of personal data had reflected the inadequacy of the enforcement power of PCPD. The proposal of granting PCPD criminal investigation and prosecution powers could meet the public expectations for enhancing deterrent measures against serious contravention of PDPO. The former PCPD advised that his team had the knowledge and experience to perform those roles efficiently and effectively. However, the discretion to prosecute or not still vested in the Secretary for Justice.

8. The Administration was of the view that in order to maintain check and balance, PCPD should not be provided with the power to carry out criminal investigations and prosecutions, and the existing arrangement under which criminal investigation and prosecution were vested respectively in the Police and the Department of Justice should be retained. The Government announced in April 2011 that proposals of granting criminal investigation and prosecution power to PCPD, empowering PCPD to award compensation to aggrieved data subjects and requiring data user to pay monetary penalty for serious contravention of DPPs under PDPO would not be implemented.

9. When the CA Panel received a briefing by PCPD on the work of his Office at its meeting on 14 February 2018, some members expressed concern that so far no successful prosecution had been brought against cyber-related contraventions of PDPO and those successful prosecutions were only related to commercial activities. These members considered that there might be a need to grant more power to PCPD in order to strengthen the protection of personal data privacy.

10. PCPD explained that where the occurrence of a security incident involved other criminal elements (e.g. access to a computer with criminal or dishonest intent), it would be referred to the Police for investigation and the criminal(s) would be charged with the more serious offence, even though certain aspects of privacy-related issues were detected in the first instance in some cases.

11. To enhance personal data privacy protection, PCPD advised that his Office had implemented a series of result-oriented promotion and education programmes to raise public awareness in this respect. The Office of PCPD had also taken the initiative to engage organizational data users of various industries with a view to assisting them in complying with PCPO through inspections, compliance checks, round-table discussions, seminars, workshops, talks and lectures.

Need for review of the Personal Data (Privacy) Ordinance to cope with new challenges

12. Members expressed concern about the collection of data and profiles of clients with the aid of advanced data processing and analytics techniques, and enquired whether such activities would be subject to regulation. Members considered that a balance should be struck between promoting businesses and the protection of personal data privacy. In response to members' concern, PCPD conceded that the rapid development of big data, artificial intelligence and related technologies in recent years had created unanticipated privacy risks and moral implications. PCPD's Office would focus on engaging the business sector in promoting the protection of personal data privacy, with a view to enhancing the culture of respect for personal data privacy in the sector. PCPD's Office would also strengthen the working relationship with overseas data protection authorities. It would explain the newly implemented rules and regulations on data protection of other jurisdictions to the local stakeholders for compliance with the requirements.

13. At the ITB Panel meeting on 12 February 2018, some members enquired whether the Administration had examined if the existing legislation was up-to-date in ensuring protection of privacy and information security in the light of the increasing prevalence of online activities, such as Internet payment and other cyber commercial activities. At the request of the ITB Panel, the Administration has provided a paper on its plan for legislative review in view of privacy and information security issues arising from the development of e-commerce, Internet of Things, Financial Technology, etc. (in **Appendix I**).

Privacy management programmes and information security of industries

14. Members expressed concern as to whether PCPD had assessed the effectiveness of the implementation of privacy management programmes with the insurance, telecommunication, banking and other sectors. PCPD advised that his Office had maintained close liaison with the relevant sectors, and talks and seminars had been organized from time to time. Through engaging the senior management of relevant industries, PCPD's Office had been promoting the concept of "Privacy by Design" among data users of relevant industries so as to safeguard privacy in the design, operation and management of any new projects/systems. Besides, relevant organizations were encouraged to conduct Privacy Impact Assessments to ensure general compliance with relevant DPPs.

15. During discussion of combating technology crimes by the Panel on Security on 6 December 2016, members noted that CSTCB was preparing a large-scale Cyber Security Drill to strengthen the overall capabilities of local critical infrastructures in responding to cyber security incidents, to enhance the

existing communications with overseas counterparts and to intensify the existing protection of the cyber environment of Hong Kong. Members sought information on how the Police would launch the Cyber Security Drill and the measures against cyber attacks at local critical infrastructures.

16. The Administration advised that there were five major sectors in the local critical infrastructures, i.e. banks and financial institutions, communication service, transport and maritime service, public utilities and government service. Assistance was provided to the operators of those critical infrastructures regarding the requirements on security, system design as well as simulation on cyber attacks. CSTCB would launch a large-scale cyber security drill in 2017 to test preparedness and response, so as to strengthen the overall capabilities of local critical infrastructures in responding to cyber security incidents.[3]

Follow-up on the loss of Registration and Electoral Office's laptop computers containing personal data of registered voters

17. Following the above incident of the Registration and Electoral Office ("REO"), members expressed grave concern about the possibility of use of the personal data of registered electors for producing forged Hong Kong Identity Cards, or by fraudsters for conducting internet banking or phone-banking transactions. According to the Administration, REO had written to Government departments and organizations of various sectors (including finance, insurance, telecommunications, retail, estate agents, information technology, etc.) to notify them of the incident and appeal to their assistance in adopting appropriate measures to prevent criminals from using the relevant information as a means of identity theft in criminal activities.

18. Members also urged the Administration to take measures against unauthorized changes of electors' registration particulars by a third party in the wake of the REO incident. The Administration advised that the information of geographical constituency electors had been encrypted in accordance with the relevant security requirements and protected by multiple encryptions. The encryption algorithm used in the system conformed to the related guideline of OGCIO, and was one of the most stringent industrial standards in use. Noting from PCPD's investigation report that REO had allowed staff to share passwords and handle passwords without extreme care, some members criticized that the way how REO handled the passwords of notebook computers had undermined their effectiveness.

[3] According to the Administration, cross-departmental cyber security drills were conducted in January 2017 and January 2018.

19. Members also took the view that the REO incident revealed that there were inadequacies in the handling of electors' personal data by REO. They urged REO to review and devise appropriate procedures in the handling of personal data of electors and related work processes. PCPD advised that in the REO incident, the claimed effectiveness of the need for storing personal data of all electors was not proportional to the associated risks. The security measures adopted by REO were not proportional to the degree of sensitivity of the data and the harm that might result from a security incident either. REO was directed to, among others, set internal guidelines in respect of the processing of personal data in all election-related activities and ensure staff's compliance with such guidelines.

20. At the ITB Panel meeting on 12 February 2018, some members enquired if OGCIO had received request from REO for assistance and whether the Administration was aware of any leakage of personal information as a result of the REO incident. According to the Administration, OGCIO had provided advice and reminded REO of the need to comply with the various information security guidelines. REO had implemented most of the recommendations and was following up on the remaining ones. So far, there was no evidence showing that personal information had been leaked following the REO incident. At the CA Panel meeting on 14 February 2018, PCPD informed members that the REO incident was still under investigation by the Police, and no complainant had ever reported actual loss to his Office in connection with the REO incident.

Relevant Legislative Council questions

21. At the Council meeting of 29 November 2017, Hon Charles MOK raised a written question on measures to enhance information security in local enterprises and industries. In particular, the Administration was asked whether the liabilities of data users would be increased in guarding against the leakage of personal data, and whether a mandatory requirement would be introduced for reporting data leakage incidents. At the Council meeting of 14 December 2016, Hon Charles MOK raised a written question on information security incidents and cybercrimes in Hong Kong. The Administration's replies to Mr MOK's questions are in **Appendices II** and **III** respectively.

Recent developments

22. The CA Panel, the ITB Panel and the Panel on Security will hold a joint meeting on 14 November 2018 to discuss the incident of leakage of passengers' personal data by Cathay Pacific Airways and issues relating to protection of personal data and cyber security.

Relevant papers

23. A list of the relevant papers on the Legislative Council website is in **Appendix IV**.

Council Business Division 2
Legislative Council Secretariat
9 November 2018

Appendix I

LC Paper No. CB(4)1522/17-18(01)

香港特別行政區政府
創新及科技局

香港添馬添美道二號
政府總部西翼二十樓

INNOVATION AND
TECHNOLOGY BUREAU

THE GOVERNMENT OF THE HONG KONG
SPECIAL ADMINISTRATIVE REGION

20/F, West Wing, Central Government Offices,
2 Tim Mei Avenue, Tamar, Hong Kong

電話 Tel: 3655 5607
圖文傳真 Fax: 3153 2664

By email

31 August 2018

Mr Daniel SIN,
Clerk to Panel,
Panel on Information Technology and Broadcasting,
Legislative Council Complex,
1 Legislative Council Road,
Central, Hong Kong

Dear Daniel,

Information requested at the meeting of the Panel on Information Technology and Broadcasting on 12 February 2018

At the meeting of the Panel on Information Technology and Broadcasting on 12 February 2018, Members requested supplementary information on the following:

(a) the Government's plan for legislative review in view of the privacy and information security issues arising from the development of e-commerce, Internet of Things (IoT), Financial Technology (FinTech), etc.; and

(b) the Government's assessment on the current cyber security situation in Hong Kong, and whether the Government would conduct victimisation surveys on cyber crimes.

In consultation with the relevant bureaux/departments, our response is set out below.

Legislative review

Regarding information security, Hong Kong has many pieces of legislation tackling computer and Internet-related crimes. For example, the Theft Ordinance (Cap. 210) deals with offences of destroying, defacing, concealing or falsifying records kept by computer; the Crimes Ordinance (Cap. 200) tackles access to computer with criminal or dishonest intent; and the Telecommunications Ordinance (Cap. 106) prohibits unauthorised access to computer by telecommunications.

Although certain laws do not mention explicitly the cyber environment, they can still apply to the virtual world. For example, the Unsolicited Electronic Messages Ordinance (Cap. 593) prohibits fraud activities related to the sending of multiple commercial electronic messages; and the Personal Data (Privacy) Ordinance (Cap. 486) is applicable to any personal data which is practicable to be accessed and processed. The Government will review the relevant laws from time to time in view of the volatile environment and amend them when necessary.

On protection of privacy, Members expressed concern over the protection of privacy of children on the Internet. The Personal Data (Privacy) Ordinance is a technology-neutral legislation and protects data subjects of all ages including children. The Office of the Privacy Commissioner for Personal Data (PCPD) has also carried out education on children's privacy by, for example, distributing information in relation to protection of personal data privacy on its main website (i.e. pcpd.org.hk) and two thematic websites (i.e. "Be SMART Online" and "Children Privacy"), and publishing guidelines for organisations, parents and teachers.

Concerning the promotion of FinTech, the Government strives to facilitate financial innovation on the one hand and to protect the investing public on the other. To this end, we keep our legislative and regulatory regime under constant review. Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC) and Insurance Authority (IA) have established their respective dedicated FinTech liaison platforms to enhance communications with the FinTech industry. HKMA, SFC and IA have also launched their respective regulatory sandboxes to allow financial institutions to test FinTech projects in a confined environment.

Assessment on the current cyber security situation and victimisation surveys on cyber crimes

The Hong Kong Police Force (HKPF) recorded 5 567 cases of technology crime in 2017 with a total financial loss of around $1.4 billion. Both figures have shown a decline when compared with 2016 (5 939 cases and $2.3 billion).

The HKPF have been closely monitoring and analysing the latest trends of technology crimes in Hong Kong and overseas, as well as maintaining close liaison with relevant law enforcement agencies and industry stakeholders with a view to timely assessing the cyber security situation in Hong Kong. Subject to the availability of resources, the HKPF will prepare and maintain statistics useful to their work depending on operational needs and the level of effectiveness. The HKPF currently has no plan to conduct victimisation surveys on technology crimes.

In addition, the Government studies the surveys and reports prepared by the industry to assess Hong Kong's cyber security situation in comparison to other areas. According to the Microsoft Security Intelligence Report in 2017, about 6.4% of computers in Hong Kong were targeted by malware, which was lower than the global average of 7.8% and much lower than the highest rate of 26.6% in Bangladesh. Furthermore, according to the Safe Cities Index 2017 published by the Economist, among the 60 cities, Hong Kong was ranked fifth in terms of digital security.

We will continue to strengthen information security within the Government and collaborate with different stakeholders to protect the public and businesses against cyber security threats with the aim of promoting Hong Kong's overall information security and cyber resilience.

Yours sincerely,

(Salina MAK)
for Secretary for Innovation and Technology

Appendix II

Press Releases

LCQ15: Measures to enhance information security
****

Following is a question by the Hon Charles Mok and a written reply by the Secretary for Innovation and Technology, Mr Nicholas W Yang, in the Legislative Council today (November 29):

Question:

Earlier on, hackers broke into the computer system of a local travel agency, encrypted the personal data of 200 000 customers stored therein and then blackmailed the agency. There are views that the crimes of hacker attacks have become increasingly serious, but the information security awareness of local enterprises is inadequate. On the other hand, quite a number of countries and regions have put in place cyber security strategies with a view to building a secure cyberspace. In this connection, will the Government inform this Council whether:

(1) the authorities will review the existing cyber resilience of the various regulated industries (e.g. banking, tourism and public utilities) and require operators of those industries to attain ISO/IEC 27001 information security management system certifications for the specific scopes of their business;

(2) whether the authorities will (i) assist local enterprises (especially small and medium enterprises) in assessing the adequacy of their information security measures and provide them with the relevant technical support, and (ii) provide them with more comprehensive training on information security, so as to enhance the levels of the information security management of those enterprises;

(3) the authorities have, for the sake of nurturing more information security talents, plans to (i) encourage more information technology practitioners to join the information security profession, (ii) collaborate with industry associations in subsidising employees to receive on-the-job training on information security and providing relevant job-matching service, and (iii) introduce measures to increase the interest of local students in joining the information security industry;

(4) the authorities will review if the Personal Data (Privacy) Ordinance (Cap. 486) is still up-to-date amid the rapid development of information technology; whether they will increase the liabilities of data users in guarding against the leakage of personal data, and introduce a mandatory requirement for reporting data leakage incidents; and

(5) the authorities will, for the sake of enhancing the cyber resilience of local enterprises, adopt the following strategies: (i) formulating the short, medium and long term specific action plans, (ii) advising and assisting various organisations to enhance their cyber security defence frameworks and recruit more information security professionals who have attained the certifications, (iii) requiring the enterprises concerned to conduct information security risk assessments, (iv) providing enterprises with training to develop their information security incident response capability, (v) strengthening information security of the supply chain, and (vi) continuously monitoring

and conducting risk assessments of the information security of local enterprises?

Reply:

President,

The Government attaches great importance to information security and cyber security. The Office of the Government Chief Information Officer (OGCIO) and its Government Computer Emergency Response Team (GovCERT) have been closely monitoring the overall cyber security situation in Hong Kong; and, in collaboration with the Cyber Security and Technology Crime Bureau (CSTCB) under the Hong Kong Police Force (HKPF) and the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) under the Hong Kong Productivity Council (HKPC), providing different stakeholders with support in relation to cyber security.

After consulting relevant bureaux and departments, our reply to the various parts of the question is as follows:

(1) Based on the business characteristics of a particular industry, relevant regulatory agencies stipulate the regulatory ambit and measures of the information system, including information and data security, risk management, response to cyber threats, contingency arrangement, recovery of business operation, etc. The OGCIO provides public and private organisations with information on internationally recognised standards on information security and practice guides through its InfoSec website, in order to facilitate them to take protective and preventive measures as appropriate according to their business needs. The OGCIO also actively keeps in view the latest development of the standard of information security management system ISO/IEC 27000 series, and regularly publishes and updates the article "An Overview of ISO/IEC 27000 family of Information Security Management System Standards" on its website for reference by the public and private organisations.

Moreover, the CSTCB is dedicated to combating technology crime, increasing the capability for handling incidents of major cyber security or large-scale cyber attacks, and conducting timely cyber threat audits and analyses so as to prevent and detect cyber attacks on critical infrastructure.

(2) and (5) Being the supporter and facilitator of information security in the community, the OGCIO has been actively collaborating with different stakeholders to provide local enterprises (including small and medium enterprises (SMEs)) with assistance in responding to information security incidents, security threat alerts, preventive guidelines and security education.

In regards to risk assessment, the HKCERT launched the SME Free Web Security Health Check Pilot Scheme jointly with various local trade associations in 2016, to help SMEs check the security measures of their websites, suggest improvement measures, and verify the effectiveness of the measures after implementation.

The Innovation and Technology Commission rolled out the Technology Voucher Programme in November 2016 to assist local SMEs in using technology services and solutions, including those targeting cyber security. SMEs can apply for subsidy for solutions defending against cyber attacks so as to minimise the risk associated with information loss and cyber security.

On the other hand, the CSTCB has been adopting a multi-agency approach in strengthening the reliability of enterprises' information system networks, as well as enhancing Hong Kong's capability of protecting relevant information system networks and resisting cyber attacks. The CSTCB will continue to detect syndicated and highly sophisticated technology crimes; carry out timely cyber threat audits and analyses; and conduct relevant thematic researches. The CSTCB also rolls out various types of projects to boost enterprises' awareness of cyber security. Examples include regularly hosting quarterly cyber security seminars since April 2016 covering different types of emerging cyber threats, as well as inviting cyber security experts to share on relevant counter-measures; partnering with the Hong Kong Monetary Authority and the Hong Kong Applied Science and Technology Research Institute to co-organise the Cyber Security Summit 2016 in which the latest local and global trends of cyber attacks were discussed; jointly launching the Cyber Security Professionals Awards Scheme with the GovCERT and the HKCERT to recognise individuals in the cyber security field for their excellent performance and promote the importance of cyber security.

(3) The Government is committed to working with the industry to nurture information security talents. We encourage tertiary institutions to provide information technology (IT) practitioners with more information security programmes; work with professional information security associations to promote professional accreditation; train up more IT practitioners with professional knowledge and skills in information security; and encourage them to join the information security profession.

Regarding on-the-job training, the HKPC, the HKCERT and the GovCERT have from time to time organised conferences, thematic seminars and workshops, including certificate courses on information security and the annual Information Security Summit, in order to enhance IT practitioners' skills and knowledge of information security.

The Government has also been actively nurturing the interests of the youth in information security through organising various activities. For example, teaming up with professional associations and Radio Television Hong Kong to conduct school visits and InfoSec Tours since 2008 to disseminate information security messages to over 62 000 teachers, students and parents; organising the Cyber Security Competition jointly with the University of Hong Kong in 2016 and 2017 to arouse students' interest in the information security profession and identify computer technology talents; and partnering with the HKPF and the HKCERT to organise the promotional event Build a Secure Cyberspace each year to enhance public understanding on information security.

(4) According to the Constitutional and Mainland Affairs Bureau, the Office of the Privacy Commissioner for Personal Data (PCPD) has been keeping a close watch on the requirements pertinent to the reporting of personal data leakage and the obligations of data processors in different jurisdictions. It is understood that, at present, only a small number of jurisdictions have mandatory requirements for data processors to report data leakage to authorities responsible for privacy or data protection. The Government has sought the public's views on the reporting mechanism for personal data leakage when conducting a review of the Personal Data (Privacy) Ordinance in 2009. Of the views

received, the majority considered a voluntary reporting mechanism more preferable. The PCPD subsequently issued the Guidance on Data Breach Handling and the Giving of Breach Notifications in June 2010, which was updated in October 2015. The PCPD will continue to keep in view the effectiveness of the current voluntary reporting mechanism.

Ends/Wednesday, November 29, 2017
Issued at HKT 12:10

NNNN

Appendix III

Press Releases

LCQ19: Information security in Hong Kong
****

Following is a question by the Hon Charles Peter Mok and a written reply by the Secretary for Innovation and Technology, Mr Nicholas W Yang, in the Legislative Council today (December 14):

Question:

In recent years, information security incidents and cybercrimes, which involved increasingly sophisticated modus operandi and technology, have occurred frequently in Hong Kong, thus putting the networks of government departments, financial system and enterprises under threats. In the first eight months of this year, the Police have received 49 reports of blackmails using encryption ransomware, and the total monetary loss involved in five of such cases was nearly $70,000. In addition, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) under the Hong Kong Productivity Council received 247 reports of blackmails using encryption ransomware over the first nine months of this year, representing a more than threefold year-on-year increase. Regarding the enhancement of the information security of government departments, the financial system and the business operations of enterprises in Hong Kong, will the Government inform this Council:

(1) whether it knows the respective numbers, in each of the past three years, of reports of incidents in which computers or websites of (i) government departments and (ii) other organisations were subject to cyberattacks and encountered information security incidents, with a breakdown by name of the department/organisation and type of incident (including web defacement, intrusion of networking and information systems, distributed denial-of-service (DDoS) attacks and blackmails using encryption ransomware);

(2) given that the computers of the Harbour Patrol Section of the Marine Department and the Office of the Centre for Food Safety of the Food and Environmental Hygiene Department had, one after another, fallen victims to implantations and intrusions by hackers in October this year, of the respective monetary losses suffered by the Government as a result of such incidents; whether the authorities have reviewed if the computer systems and anti-virus software in use by various government departments are adequate to guard against cyberattacks, such as phishing websites, botnets, malicious software and DDoS attacks;

(3) given that the server of the Immunisation Record System of the Clinical Information Management System (CIMS) of the Department of Health was earlier suspected of having been intruded into by hackers, how the authorities will enhance the security of CIMS to protect the personal data and privacy of members of the public;

(4) given that the Office of the Government Chief Information Officer (OGCIO) has indicated its plan to strengthen its efforts to defend against cyber threats by forming a new team in the middle of this year, (i) whether that team has been formed, (ii) what specific tasks the team has undertaken and has planned to undertake respectively, and (iii) whether the team will conduct

information security assessments and audits for various government departments; if the team will, of the timetable; if not, the reasons for that;

(5) of the number of cyber security drills conducted by the Government Computer Emergency Response Team Hong Kong in collaboration with the Hong Kong Police Force (HKPF) since its establishment, and the respective categories and scales of the simulated cyberattack incidents (set out separately in chronological order);

(6) of the scope of work of the Cyber Security and Technology Crime Bureau (CSTCB) of the HKPF in addressing cybercrimes; whether CSTCB has participated in the various types of information security work of the Security Bureau, the Innovation and Technology Bureau and OGCIO, including (i) the conduct of security risk assessments and audits, (ii) the implementation of technical security solutions, and (iii) the upgrade of security infrastructures;

(7) how many organisations participated in the SME Free Web Security Health Check Pilot Scheme organised by the authorities through HKCERT this year; whether and how the authorities have assessed the effectiveness of the scheme, and whether they will expand the scheme to enable more small and medium enterprises (SMEs) to participate; given that SMEs face higher information security risks, whether the Government will provide SMEs with extra funding and support to help them strengthen the security of network infrastructure and enhance information security;

(8) given that a large-scale cyberattack launched by hackers in the United States in October this year has rendered a number of major local websites paralysed, whether the authorities have formulated an information security strategy in relation to the promotion of smart city development in Hong Kong, so as to address cyberattacks targeting household, personal and mobile network devices, merchant point-of-sale systems and Internet-of-Things systems;

(9) given that incidents of hacker intrusions into automatic teller machine systems of banks have occurred successively in Thailand and Taiwan recently, whether the authorities have specific measures in place to safeguard the information security of the financial system of Hong Kong so as to ensure that the system has adequate protection against similar incidents of hacker intrusions; whether they will conduct comprehensive risk assessments on the current information security of government agencies, financial institutions, industry bodies (such as telecommunication companies) and their infrastructures;

(10) whether the authorities have assessed Hong Kong's long-term needs for information security personnel to tie in with the direction of smart city and financial technology development in Hong Kong; whether they have plans to formulate policies to nurture information technology personnel and network security experts, so as to address various types of information security threats; and

(11) since the review of the current legislation and the relevant administrative measures in 2000, whether the authorities have plans to establish afresh an inter-departmental working group for the enhancement of information security work to study ways to address the new challenges posed by the application of cloud technology?

Reply:

President,

With the rapid development of information technology (IT) and increasing popularity of smart devices, information security and the threats posed by cyber attacks have brought impacts on internet users. The Government has been closely monitoring the trend of cyber attacks and related security threats. The Office of the Government Chief Information Officer (OGCIO) has been collecting cyber threat information disseminated by the cyber security industry and computer emergency response teams around the world, and issue timely security alerts and reminders to Government bureaux and departments (B/Ds), as well as assist government IT management staff and Information Security Incidents Response Teams in B/Ds to make prompt response and strengthen their precautionary measures.

Having consulted the Security Bureau (SB), the Commerce and Economic Development Bureau (CEDB), the Financial Services and the Treasury Bureau (FSTB) and other relevant departments, the reply to each part of the question is as follows:

(1) In the past three years, OGCIO received a total of 31 information security incident reports from government departments, while the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) received a total of 13 517 such reports from local enterprises and users over the same period. The relevant incidents by type are set out in Annex.

(2) Regarding the hacker intrusion incident at the Harbour Patrol Section of the Marine Department and the office of the Centre for Food Safety of the Food and Environmental Hygiene Department, the departments concerned have promptly and properly dealt with the incidents in accordance with the established information security incident response mechanism and procedures. As the intrusions were caused by ransomware, OGCIO also immediately issued reminders and guidelines on strengthening ransomware prevention to B/Ds, requesting them to step up checks on the computer systems and anti-malware softwares, so as to ensure the information security defensive capabilities within the Government. The Government has not suffered any monetary loss as a result of the relevant incidents.

On protecting government information systems and networks, the Government has put in place overall management framework, technical measures and security mechanisms to closely monitor the operation of government information and network systems, so as to detect and block various kinds of potential cyber attacks. B/Ds should abide by the Government's information security policies and guidelines, take appropriate measures to ensure the safe and normal operation of the Government's information and network systems, including the implementation of multiple layers of security such as the use of firewalls, intrusion detection and defensive systems and anti-malware softwares. B/Ds should also ensure the correct set-up of systems and the timely installation of security patches to prevent any security vulnerabilities from posing threats against the Government's information systems. Moreover, they should conduct regular security risk assessments and third-party audits on their information and network systems, to ensure that the systems comply with the relevant security requirements and regulations, and have adequate defensive capabilities to protect government systems and data assets.

In addition, OGCIO has been closely monitoring the trends of cyber attacks and the associated security threats, providing timely technical assistance and recommending precautionary measures to B/Ds. It also issues technical guidelines, security alerts and reminders and organises seminars to strengthen their information security awareness and capabilities to prevent, detect and respond to cyber attacks.

(3) In July 2016, the Department of Health (DH) discovered that the Immunisation Record System of its Clinical Information Management System had been intruded by hackers. DH handled the incident in accordance with the established procedures, reported the incident to OGCIO and the Office of the Privacy Commissioner for Personal Data, and referred the case to the Police for investigation. The DH also sent letters to all those who might be affected, advising them to be vigilant against any illegal use of their personal information.

On the protection of personal and classified information, the Government has put in place very stringent information security requirements and responsive measures, stipulating that the access to and use of relevant application systems and data should be restricted to authorised persons and that data access rights should be clearly defined and reviewed periodically. It is also required that sensitive data and documents, when being saved or transmitted, should be encrypted in accordance with recognised industry standards to ensure the proper protection of government data assets.

In 2016, OGCIO conducted a comprehensive review on the Government IT Security Policy and Guidelines, by making reference to the latest ISO 27001 international standards and other industry best practices, in order to strengthen the security requirements in individual areas, including the confidentiality requirements for storing sensitive information and departmental management capability to respond to information security incidents.

(4) OGCIO set up a new team in July this year to step up actions against cyber security threats. The team is establishing a pilot cyber threat information sharing platform, which will collate and evaluate cyber threat information and data from different sources using big data analytics technology, so that more targeted cyber threat alerts can be issued to B/Ds and provide them with advice on counter measures. Moreover, OGCIO will launch a new round of "security compliance audits" by the end of this year to assess B/Ds’ compliance with the Government IT Security Policy and Guidelines. During the course of assessment, OGCIO will assist relevant B/Ds to continuously improve their security management systems and to cope with emerging security threats.

(5) Since 2014, the Hong Kong Police Force (HKPF) has conducted various types of cyber security drills together with industry stakeholders and local critical infrastructures. In 2014, a total of 14 organisations of critical infrastructures participated in the drills. In 2015, the number of participating organisations increased to 28. Through various simulated incident scenarios, cyber security drills test the capabilities of incident analysis, the standing incident response procedures and the communication protocol of the participants. The simulated cyber attacks incidents include the most common scenarios with profound impacts, such as distributed denial-of-service attacks, web defacement, intrusion of network and information systems,

ransomware, malware and sensitive data breaches.

The Police will, in collaboration with OGCIO, conduct a large-scale cyber security drill involving 30 government departments in January 2017 to enhance government departments' capability to protect information systems and handle cyber security incidents.

(6) The Cyber Security and Technology Crime Bureau (CSTCB) of HKPF is responsible for a wide range of duties in tackling cyber crimes. Its major functions include:

(a) detecting syndicated and highly sophisticated technology crimes and conducting proactive intelligence-led investigations;
(b) providing assistance to critical infrastructures by conducting timely cyber threat audits and analyses to prevent and detect cyber attacks against them;
(c) enhancing incident response capability to major cyber security incidents or massive cyber attacks;
(d) strengthening thematic researches on cyber crime trend and mode of operation, vulnerabilities of computer systems and development of malware;
(e) strengthening co-operation with local and overseas stakeholders and law enforcement agencies to counter prevalent technology crimes and cyber threats; and
(f) conducting trainings on cyber security and technology crimes.

Since its establishment, CSTCB has been collaborating with various government departments and stakeholders of different trades to strengthen the reliability of the information system network of critical infrastructures, as well as to enhance Hong Kong's capability to protect relevant information system networks and guard against cyber attacks.

(7) To enhance the cyber security awareness among local small and medium enterprises (SMEs) and strengthen their defensive capabilities against cyber attacks, HKCERT launched the SME Free Web Security Health Check Pilot Scheme jointly with a number of local trade associations early this year to check the health status of SMEs' websites and suggest improvement measures, and to verify the effectiveness of the measures upon implementation. The first round of checks under the scheme was completed in the middle of this year, and website security check reports and free consultation services were provided to 30 participating SMEs. In August, seminars were held to share the findings and improvement suggestions. A second round of checks has also been completed. Through the scheme, participating SMEs can have a better understanding of the security risks of their websites and the best practices in website security, thereby enhancing the protection for their websites. OGCIO will continue to work closely with HKCERT to explore activities which will further raise the cyber security level of local SMEs.

The Innovation and Technology Commission launched a $500 million Technology Voucher Programme on a pilot basis under the Innovation and Technology Fund on November 21 to subsidise the use of technological services and solutions by SMEs, including IT that assists enterprises to enhance cyber security.

(8) In the process of promoting the development of smart city, it is imperative to develop relevant IT security and technical standards. When considering the options for implementing Internet of Things, the Government will evaluate the security risks in the relevant segments, including terminal devices, network systems,

information management, etc, in order to comply with the requirements under the security regulations and policies of the Government. We are conducting a consultancy study for formulating a Smart City Blueprint for Hong Kong, including the development of IT security and technical standards. The study is expected to complete in mid-2017.

(9) The Hong Kong Monetary Authority (HKMA), the banking industry and HKPF have been monitoring the crime cases related to ATMs, including the cases involving overseas ATMs being intruded by hackers, causing them to dispense cash automatically.

According to information provided by HKMA, these cases involved the planting of malwares into the overseas ATMs in respect of which no protective measures against malwares have been implemented. In Hong Kong, effective security measures against malwares have been implemented in all ATMs in accordance with HKMA's guidelines. In light of these cases, HKMA, the banking industry and HKPF have earlier reminded banks to review their security controls, so as to further reduce the risk of local ATMs being hacked.

To strengthen the cyber resilience of the banking sector in Hong Kong, HKMA announced in May 2016 the launching of Cybersecurity Fortification Initiative (CFI), which is underpinned by three pillars:

(a) Cyber Resilience Assessment Framework: the assessment framework aims at assessing an authorised institution (AI)'s cyber risk exposure and cyber resilience. The results will form a basis for an improvement plan for cyber resilience. It also allows HKMA to get a holistic view of the preparedness of individual AIs, as well as the entire banking sector, in cyber security;

(b) Professional Development Programme: the Professional Development Programme is a localised certification scheme and training programme developed by HKMA together with the Hong Kong Institute of Bankers and the Hong Kong Applied Science and Technology Research Institute (ASTRI). The aim of launching this integrated and well-structured programme is to train and nurture cyber security practitioners in the AIs and the IT industry, so as to enhance their cyber security awareness and technical capabilities to conduct cyber resilience assessments and simulation testing; and

(c) Cyber Intelligence Sharing Platform: the Cyber Intelligence Sharing Platform is jointly implemented by HKMA and the Hong Kong Association of Banks (HKAB) to support the implementation of simulation testing and facilitate the sharing of cyber intelligence among AIs. Relevant cyber intelligence sourced from different reliable channels will be collected, analysed and shared on this platform together with detailed cyber-threat analysis report and recommendations. Through this platform, member banks of HKAB will be able to tap the latest threat scenarios and get prepared accordingly.

With the support of the banking industry and other stakeholders, the HKMA has made good progress in implementing the CFI. The three pillars are expected to be formally rolled out in December 2016.

Furthermore, CSTCB has been endeavouring to facilitate the sharing of cyber-attack intelligence in the financial sector of

Hong Kong. CSTCB is planning to establish a Cyber-attack Intelligence Sharing Platform to address dynamic cyber threat and the increasingly complex cyber attacks, as well as to share intelligence on cyber attacks.

In May this year, HKPF, HKMA and ASTRI co-organised Cyber Security Summit 2016, which was a three-day event with supervisors of financial institutions, regulatory bodies and technology solution providers among its guests. The summit shared the latest local and global trends of cyber attacks, and enhanced the awareness and preparedness of important professional bodies and critical infrastructures in Hong Kong in response to cyber security incidents and hacker attacks.

As regards telecommunications operators, according to information provided by CEDB, they are required to ensure the effective operation of their networks to maintain and provide satisfactory services in accordance to the licence conditions.

(10) According to the statistics by the Information Systems Audit and Control Association, there are 2 327 Certified Information System Auditors and 474 Certified Information Security Managers in Hong Kong as at September 2016. Moreover, information of the International Information Systems Security Certification Consortium, Inc shows that a total of 1 413 local practitioners have acquired the qualification of Certified Information Systems Security Professional. To address the information security threats faced by Hong Kong, the Government will continue to collaborate with schools and the education sector (including tertiary institution) to enrich IT-related disciplines with information security programmes. The Government will also work with professional associations of information security to promote professional accreditation for IT practitioners so as to train up more IT practitioners with professional knowledge and skills in information security, and to facilitate the development of relevant manpower resources.

(11) The Government has formulated a set of comprehensive Government IT Security Policy and Guidelines which is subject to regular reviews, in order to address challenges brought by the Government's use of cloud and other IT developments.

Ends/Wednesday, December 14, 2016
Issued at HKT 16:15

NNNN

Annex

Reports of Information Security Incidents Received by OGCIO

Information security incident	**2014-15**	**2015-16**	**2016-17 (As at October 2016)**
Website defacement	2	2	1
Unauthorised access	2	1	2
Denial-of-service attack	6	2	-
Ransomware	-	-	3
Others (including fraudulent email, malware infection, loss of mobile device, data leakage, etc)	5	1	4
Total	**15**	**6**	**10**
B/Ds involved	13	5	10

Reports of Information Security Incidents Received by HKCERT

Computer security incident	**2014**	**2015**	**2016 (As at October)**
Hacking/website defacement	146	151	76
Distributed denial-of-service attacks	125	130	94
Ransomware	-	51	278
Phishing	594	1 978	1 635
Botnets	1 973	1 943	1 611
Malware (excluding ransomware)	298	226	787
Other computer security incidents (including identity theft, data leakage, unauthorised access, etc)	307	449	665
Total	**3 443**	**4 928**	**5 146**

Appendix IV

Relevant documents on issues relating to protection of personal data and cyber security

Committee	Date of meeting	Paper
Panel on Constitutional Affairs ("CA Panel")	15.11.2010 (Item IV)	Agenda Minutes
	20.11.2010 (Item I)	Agenda Minutes
Panel on Security	6.12.2016 (Item V)	Agenda Minutes
Panel on Information Technology and Broadcasting ("ITB Panel")	12.12.2016 (Item V)	Agenda Minutes
Legislative Council ("LegCo")	14.12.2016	Official Record of Proceedings Pages 144 – 155 (Written question)
CA Panel	20.3.2017 (Item V)	Agenda Minutes
	11.4.2017 (Item I)	Agenda Minutes
	19.6.2017 (Item V)	Agenda Minutes
LegCo	29.11.2017	Official Record of Proceedings Pages 116 – 120 (Written question)
ITB Panel	12.2.2018 (Item V)	Agenda Minutes
CA Panel	14.2.2018 (Item IV)	Agenda Minutes

Committee	**Date of meeting**	**Paper**
LegCo	28.2.2018	Official Record of Proceedings Pages 73 – 76 (Written question)

Council Business Division 2
Legislative Council Secretariat
9 November 2018