LCQ2: Enhancing information security and the protection for privacy of personal data

Following is a question by the Hon Charles Peter Mok and a reply by the Secretary for Constitutional and Mainland Affairs, Mr Patrick Nip, in the Legislative Council today (November 14):

Question:

In recent years, incidents involving massive leakage of personal data by government departments and private organisations have occurred frequently. Not until half a year after learning of the leakage of the data of about 9.4 million passengers did an airline announced it last month. In addition, in less than a month after the launch of the Faster Payment System, a number of fraud cases occurred in which the fraudsters committed crimes by making use of the personal data of members of the public and taking advantage of the loopholes in the process of setting up direct debit authorisation by electronic wallets users, thereby causing financial losses to the members of the public. On enhancing information security and the protection for privacy of personal data, will the Government inform this Council:

(1) whether it will, by making reference to the General Data Protection Regulation of the European Union, study prescribing in the Personal Data (Privacy) Ordinance the obligations of data processors, and that data users are required, in the event of data leakage incidents, to notify the Office of the Privacy Commissioner for Personal Data and the data subjects within specified time limits; and

(2) whether it will comprehensively assess the information security risks currently faced by government departments, industries such as finance and telecommunications as well as public utilities, formulate a cross-sector information security strategy, and step up the training for information security talents (e.g. by setting up a specialised college)?

Reply:

President,

Regarding the respective parts of the question raised by Hon Charles Mok on enhancing the protection of personal data privacy and capability of responding to information security risks, our reply in consultation with the Innovation and Technology Bureau (ITB) and the Security Bureau (SB) is as follows:

(1) The Personal Data (Privacy) Ordinance (PDPO) was enacted in 1995 and has been in operation since 1996. Subsequent to the public consultation on the PDPO and the relevant legislative amendments conducted by the Government

between 2009 and 2010, the Personal Data (Privacy) (Amendment) Bill was introduced in the Legislative Council (LegCo) in 2011 and was passed by LegCo in June 2012.

During the above-mentioned consultation exercise on the PDPO, one of the issues for consultation was the personal data breach notification system. The primary consideration on the issue back then was whether a notification system should be instituted to require relevant organisations to notify the Office of the Privacy Commissioner for Personal Data (PCPD) and the affected individuals in the event of a personal data leakage, so that they could take measures to mitigate the risks posed by the data leakage, and whether the notification system should be voluntary or mandatory. Of the public views received, about half were in support of a voluntary notification system, while around one-quarter favoured a mandatory notification system. Respondents who supported a voluntary system considered that a mandatory system would impose undue burden on data users. Taking into consideration the possible impact of implementing a mandatory notification system, the Government decided to start with a voluntary notification system. To assist data users in giving data breach notifications, the PCPD issued the "Guidance on Data Breach Handling and the Giving of Breach Notifications" (Guidance) in June 2010, and subsequently made amendments to the Guidance in October 2015. The Guidance issued by the PCPD provides guidance and assistance to data users on the steps to be taken in handling data breaches. A data breach notification form is also attached to the Guidance to make it more convenient for data users to give notifications.

The Government and the PCPD noted that in the light of rapid development and wide use of technology in recent years, the processing of personal data has become massive and digitalised, resulting in higher risk posed to data users and owners as the amount of data involved in personal data leakage incidents has increased. There are views that this Cathay Pacific incident has revealed that there is room for refining and enhancing the PDPO. In this connection, the Constitutional and Mainland Affairs Bureau will keep close watch on the PCPD's investigation results and recommendations regarding the incident. Meanwhile, we have started a review in collaboration with the PCPD on the stipulations and penalties under the PDPO. While noting that there are views calling for the requirement for data users to give timely notification in data breach incidents, we are also aware of concerns in some quarters on how "data breach" should be defined, as well as the compliance capability and operational costs of businesses. We will examine carefully how the regulation of data protection and the notification arrangements could be enhanced.

(2) To protect government's information systems and data assets, having made reference to international standards, the Office of the Government Chief Information Officer (OGCIO) has formulated a comprehensive set of "Government IT Security Policy and Guidelines" (Policy & Guidelines) which covers many different aspects including security requirements for information security management framework and human resources, protection and encryption requirements for information systems and data assets, connection and access control, network and outsourcing service security, incident response and recovery, etc. OGCIO will conduct regular audits to ensure that all

departments comply with the Policy & Guidelines, as well as review and update the Policy & Guidelines from time to time to address the ever-changing cyber threats.

For infrastructure facilities owned by key industries and organisations and those not owned by government, the relevant regulatory bodies will formulate regulatory measures. In view of their unique business nature, the information security strategy, incident response and business recovery arrangements formulated by different industries vary. Industries can make reference to the Policy & Guidelines available at OGCIO's website in developing information security policies and measures that meet their needs. When necessary, OGCIO will also exchange views with the relevant regulatory bodies and give advice.

Furthermore, OGCIO, the Cyber Security and Technology Crime Bureau (CSTCB) under the Hong Kong Police Force and the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) work closely to provide cyber security related information and support to different stakeholders including government departments, key industries and organisations, and the general public, as well as publish information on major incidents and recommend preventive and remedial measures. To prevent and combat technology crimes, CSTCB has been dedicated to help enhancing critical infrastructure operators' awareness to cyber security, and their capability in handling cyber security incidents; and conducting timely cyber threat audits and analyses so as to prevent and detect cyber attacks on critical infrastructure.

For the industries, HKCERT works with industry associations to promote cyber security awareness and best practices in different sectors, as well as provide public and private organisations and the public with news on information security incidents, guidelines for defence against cyber threats and support services. OGCIO also implements the cross-sector "Cyber Security Information Sharing Collaborative Platform" to exchange information with public and private organisations as well as cyber security experts, and share risk mitigation measures, so as to more effectively enhance the overall cyber security in Hong Kong. CSTCB has also been hosting quarterly cyber security seminars to strengthen the overall defensive capabilities of such service sectors as banking and finance, transport and aviation, communications, public utility and government services in handling cyber security incidents.

Since 2014, the CSTCB has been conducting various types of cyber security drills together with industry stakeholders and local critical infrastructures. 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 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. In addition, CSTCB co-organised in January 2018 the second Inter-departmental Cyber Security Drill with the Government Computer Emergency Response Team Hong Kong, in which 40 government bureaux and departments, through different scenarios of simulated cyber attacks, strengthened their cooperation in cyber security and capabilities in

emergency response.

On education work, OGCIO and CSTCB also join hands with HKCERT to proactively promote the nurturing of talents in cyber security professionals, and co-organise activities with different organisations, such as the Cyber Security Professionals Award, cloud security professional certification seminars and Information Security Summit to enhance the information security knowledge and skills of IT practitioners. The Government also encourages tertiary institutions to strengthen information security modules in their IT-related programmes, and promote information security education in primary and secondary schools to cultivate the youth's interest in and concern about information security.

Thank you, President.