LCQ9: Data security

Following is a question by the Hon Chan Chun-ying and a written reply by the Secretary for Innovation and Technology, Mr Alfred Sit, in the Legislative Council today (August 25):

Question:

On June 10 this year, the Standing Committee of the National People's Congress passed the Data Security Law of the People's Republic of China (DSL), which will come into force on September 1. In this connection, will the Government inform this Council:

(1) as Article 21 of DSL provides that the State is to establish a categorised and hierarchical system for data protection, and the relevant departments are to draw up catalogues of important data and conduct priority protection for those data listed in such catalogues, whether the Government has considered establishing a similar data protection system in Hong Kong; if so, of the details; if not, the reasons for that;

(2) as Article 22 of DSL provides that the State is to establish centralised, uniform, highly effective and authoritative mechanisms on risk assessment, reporting, information sharing, monitoring and early warnings in respect of data security, and the relevant departments are to strengthen the work on acquisition, analyses, assessment and early warnings in respect of information on data security risks, whether the Government has considered establishing similar mechanisms for monitoring data security in Hong Kong; if so, of the details; if not, the reasons for that; and

(3) as Article 23 of DSL provides that the State is to establish a data security emergency response system, and when data security incidents have occurred, the departments responsible shall take corresponding emergency response measures, whether the Government has considered establishing a similar emergency response system in Hong Kong; if so, of the details; if not, the reasons for that?

Reply:

President,

Having consulted the Security Bureau, our consolidated reply is as follows:

The Government has formulated a set of comprehensive government information security incident response mechanism and related measures. Established by the Security Bureau, the Security Regulations include dedicated chapters governing information security for ensuring the security of government internal information and information systems. Among other things, the Security Regulations define the security classification of government information and explicitly requires government departments to properly classify the information they hold, and take corresponding measures according to the classification to ensure that the information is fully protected in the course of storage and business operations. For example, limit access to classified information or access and use of related information systems and data by authorised persons only, encrypt classified information stored in the information systems, etc. Details of the information classification and security measures are not suitable for disclosure due to security reasons.

On the other hand, the Office of the Government Chief Information Officer (OGCIO) has also formulated a set of detailed Government IT Security Policy and Guidelines (Policy and Guidelines) under the framework of the Security Regulations for compliance by all departments. The Policy and Guidelines requires all departments to explicitly define and regularly review the access rights of relevant information systems and data, set out technical requirements for the use of encryption, and stipulate that departments must establish information security management framework in order to effectively handle security matters, etc. The Policy and Guidelines also stipulates that departments must regularly conduct independent security risk assessments and audits for their information systems and data security so as to strengthen security measures. In order to raise the Government's awareness of the latest situation and response capabilities in tackling cyber risks, the OGCIO has implemented the Cyber Risk Information Sharing Platform within the Government, which utilises big data analytics technology to collect, collate and analyse information on cyber and data security threats from different sources for timely dissemination of threat alerts to all departments.

In accordance with the Policy and Guidelines, all departments have established an information security incident response team to handle their information security incidents. Both the Security Regulations and the Policy and Guidelines are developed with reference to international standards and will be reviewed and updated from time to time to tackle the latest security threats. All government departments must also abide strictly by the Security Regulations and the Policy and Guidelines mentioned above to ensure the security of government information and information systems. The OGCIO regularly conducts compliance audits for departments to ensure their information systems are compliant with relevant security requirements.

The OGCIO has also established a computer emergency response team within the Government to assist and co-ordinate departments in dealing with computer emergency response and incidents. In addition, the OGCIO organises annual Inter-departmental Cyber Security Drill to strengthen the capability of government departments in defending and responding to cyber security incidents.

In face of the security risks associated with critical infrastructures of different industries, the Hong Kong Police Force (HKPF) has established the Critical Infrastructure Security Coordination Centre (CISCC), which sought to strengthen self-protection and self-restoration capabilities of these infrastructures through public-private co-operation, risk management, on-site security inspections, promotion of restoration plans and security designs. On cyber security, the Cyber Security Centre (CSC) under the Cyber Security and Technology Crime Bureau of the HKPF provides support to critical infrastructures by conducting timely cyber threat audits and analyses to prevent and detect cyber attacks against them. The CISCC and the CSC operate round the clock to provide appropriate support to local critical infrastructures.

Meanwhile, the Government has attached great importance to co-operation and information sharing with the Mainland and international counterparts in cyber security. The OGCIO and the Bureau of Cyber Security of Cyberspace Administration of China reached a consensus on co-operation in 2016 to strengthen co-ordination and promote exchanges and co-operation in cyber security between the Mainland and Hong Kong. The OGCIO also works with the National Computer Network Emergency Response Technical Team/Coordination Center of China to obtain related cyber security vulnerability information in a timely manner through the China National Vulnerability Database and arrange preventive measures. At the international level, the OGCIO maintains close liaison with global leading computer emergency incident response organisations and computer emergency response teams in order to quickly get hold of cyber security information and prevent cyber attacks in a timely manner.

The Government will regularly review the Government's prevailing information security incident response and handling arrangements, and recommend improvement measures to continuously update and strengthen the Government's response capabilities in handling information security and incidents.