LCQ17: Enhancing cyber security

Following is a question by Prof the Hon William Wong and a written reply by the Acting Secretary for Innovation, Technology and Industry, Ms Lillian Cheong, in the Legislative Council today (October 18):

Question:

There are views pointing out that the recent spate of hacker intrusions into the computer systems of public organisations have reflected the existence of loopholes in the network security of public organisations. On the other hand, the Secretary for Innovation, Technology and Industry has indicated earlier on that the Government is conducting relevant studies on a cyber security law. In this connection, will the Government inform this Council:

(1) following the hacking of the computer systems of the Cyberport and the Consumer Council, whether the Government has instructed various public organisations to conduct immediate and regular information security checks on their computer systems to eliminate potential risks;

(2) whether the information technology security policies, standards, guidelines, procedures and relevant practice guides formulated by the Office of the Government Chief Information Officer (OGCIO) are applicable to public organisations; if so, whether OGCIO will conduct regular inspections to ensure that public organisations strictly implement such policies and guidelines, etc.;

(3) as there are views that compliance with the aforesaid policies and guidelines, etc., by public organisations necessitates computer systems of a very high standard and rather stringent daily maintenance requirements, whether the authorities have provided sufficient dedicated funding to various public organisations to carry out work on upgrading their computer systems and enhancing, among others, the management systems, defence facilities, training and education, as well as inspection and supervision relating to computer system information security; whether the authorities will, in the light of the recent incidents of hacker intrusions, increase the relevant funding for various public organisations;

(4) of the progress of enacting the cyber security law and when it is expected to be introduced into this Council for scrutiny;

(5) as it is learnt that Singapore set up the Public Sector Data Security Review Committee in 2019 to review government measures on protecting citizens' data, whether the authorities will, by drawing reference from the practice of Singapore, set up a committee on information security prior to the introduction of the cyber security law and invite relevant experts to participate in the committee, so as to regularly review the performance of government departments and public organisations in the aspects of the

management, supervision and coordination of information security; and

(6) in order to prevent intrusion by international hackers, whether the authorities will consider setting up a data bureau to comprehensively establish a data governance system, so as to build a complete cyber security barrier for Hong Kong and the country?

Reply:

President,

Having consulted the Security Bureau, reply to the questions raised by Prof the Hon William Wong is as follows:

(1) The Government is deeply concerned about the recent incidents of unauthorised access into computer systems of individual public organisations by hackers. These incidents suggest that cybersecurity threats are increasingly commonplace. All sectors of society must take effective measures to safeguard their systems and enhance security of the networks and data.

Immediately following the recent cybersecurity incidents in public organisations, the Office of the Government Chief Information Officer (OGCIO) had issued reminders to all bureaux/departments (B/Ds) of the relevant security guidelines, offered technical support, and requested B/Ds including public organisations under their purview to assess and strengthen their current information security and cybersecurity measures without further ado, in order to guard against cyberattacks and minimise the potential security risks.

(2) The OGCIO has formulated a set of comprehensive Government IT Security Policy and Guidelines (Policy and Guidelines), setting out the requirements for establishing, implementing, maintaining and continuously improving the information security management system for all B/Ds to follow. The Policy and Guidelines are timely updated by the OGCIO with reference to the latest national and international standards on information security management and industry best practices. To raise the awareness of information security risks of all B/Ds, the OGCIO also regularly reminds B/Ds to adopt effective security measures to protect government information systems and data.

While the above-mentioned policy, guidelines and government information security requirements are aimed for compliance by B/Ds, the OGCIO has uploaded the Policy and Guidelines to the Internet for reference by all public and private organisations. Individual organisations may adopt those principles and measures on security risk management recommended in the Policy and Guidelines having regard to their own circumstances.

(3) Public organisations can formulate and adopt computer systems, IT governance policies and cybersecurity defense measures that suit their own business nature, operating modes and computing facilities. They may also consider and plan for enhancing their IT infrastructure based on their actual circumstances and the latest technology development, with a view to better

managing their business needs and associated risks. B/Ds will also request public organisations under their purview to review and step up their information security and cybersecurity measures as appropriate.

(4) To enhance the protection of cybersecurity of critical infrastructures, the Government plans to define clearly, through legislation, the cybersecurity obligations of the operators of these critical infrastructure. This includes the establishment of a good preventive management system to ensure the secure operation of their information systems and networks. The Government is working on the draft legislative framework and soliciting initial views from the industry. The next step is to consult the Panel on Security of the Legislative Council and the public on the legislative proposals.

On the other hand, the Law Reform Commission (LRC) set up a sub-committee in 2019 to conduct a study on cybercrime. At the first stage, a public consultation exercise on cyber-dependent crimes and jurisdictional issues was completed in October 2022. Upon the LRC's release of a report on the topic, the Government will study the recommendations made in the report and consider follow-up actions to further enhance cybersecurity.

(5) and (6) To our understanding, the Singapore's Public Sector Data Security Review Committee is tasked to make recommendations to the Government covering areas such as strengthening data protection, incident detection and handling capabilities; as well as civil servants' awareness and ability to protect data, data protection responsibilities and governance structure. On the other hand, the National Data Bureau is taking forward the development of digital infrastructure, the opening, sharing and security of data, and digital economy, etc.

In Hong Kong, the Government has devised multi-pronged security measures and implementation mechanisms on data security risk management, covering data protection, audit and risk assessment, incident handling and response, education and training, etc., thereby safeguarding the security of government information systems and data on all fronts. As a core member of the Government's Information Security Management Committee, the OGCIO regularly conducts independent compliance audits for B/Ds to ensure their adherence to relevant security regulations, and provides guidance to B/Ds for continuous improvement of their security management systems. The OGCIO has also established the Government Computer Emergency Response Team Hong Kong (GovCERT.HK) which provides assistance and coordinates departments in dealing with computer emergency response and incidents. In addition, the OGCIO has implemented the Cyber Risk Information Sharing Platform within the Government to timely disseminate cyber and data security threats alerts to all departments. Moreover, the GovCERT.HK and the Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force co-organise the Inter-Departmental Cyber Security Drill to strengthen the capability of B/Ds in defending and responding to cybersecurity incidents.

Apart from the above, to enhance the overall information security awareness in the community, including public and private organisations, and

strengthen their capability in defending against cybersecurity threats and response to cybersecurity incidents, the OGCIO works closely with stakeholders, including the Hong Kong Internet Registration Corporation Limited (HKIRC), to administer the cybersecurity information sharing and collaborative programme "Cybersec Infohub" that promotes cybersecurity information sharing among public and private organisations, and supports the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) which offers incident response services for information security, security threat alerts, preventive guidelines and security education. In collaboration with the CSTCB, the HKIRC and the HKCERT, the OGCIO also organises various publicity campaigns and training to remind the community to strengthen their cybersecurity measures and protect their information systems and data against cyberattacks.

It is the Government's ongoing effort to review and strengthen the responses of Government and all sectors of society against information security risks and fortify the data security protection. As mentioned above, the Government will make reference to the latest information security management standards and industry's best practice and timely update the Policy and Guidelines for B/Ds' compliance and reference by the public. We are also formulating a legislative framework to enhance the cybersecurity protection of critical infrastructures. The Government will continue to press ahead with relevant work and review from time to time, in a bid to build Hong Kong into a safe and secure smart city.