# LCQ7: Information security measures of the Government

Following is a question by the Hon Yung Hoi-yan and a written reply by the Secretary for Innovation and Technology, Mr Nicholas W Yang, in the Legislative Council today (April 22):

Question:

On the 22nd of February this year, a newspaper reported the content of a report on the anti-epidemic work of Hong Kong, which had purportedly been prepared by the Chief Executive's Office and submitted to the Central Authorities. Given that this type of documents should be highly confidential in nature, some members of the public are worried that there are serious loopholes in the Government's information security measures. In this connection, will the Government inform this Council:

(1) of the number of incidents, uncovered since January 2015 by the Government, of suspected violations of the relevant laws or codes on information security by some people that resulted in the leakage of information, and set out one by one in a table such incidents' causes (e.g. intrusion into its information systems by hackers, and negligence or deliberate divulgence by some people) and their impacts, as well as the follow-up measures taken by the Government and the effectiveness of such measures;

(2) of the government departments and post titles of the officers responsible for conducting investigations into the incidents mentioned in (1), the details of the investigation work and the follow-up actions, as well as the circumstances under which the investigation results will be made public; and

(3) whether it will, in the light of information leakage incidents, conduct a comprehensive review on the existing measures and mechanism on information security; if so, of the details; if not, the reasons for that?

Reply:

President,

The Government all along attaches great importance to information and cyber security. The Office of the Government Chief Information Officer (OGCIO) together with the Security Bureau have formulated a set of comprehensive Government IT Security Policy and Guidelines (Policy and Guidelines), covering management framework, policies and technical measures for bureaux and departments (B/Ds) to follow and use in order to properly protect information systems and prevent leakage of information to unauthorised persons. In doing so, OGCIO made reference to international best practices, such as the International Organisation for Standardisation

(ISO)/International Electrotechnical Commission (IEC) 27001 standard. In addition, OGCIO regularly audits the compliance of B/Ds to ensure that their information systems and network facilities meet the security requirements.

Our consolidated reply to the questions is set out below –

Since January 2015, OGCIO has received a total of 19 information security incident reports that might involve leakage of information possessed by the government. A breakdown of the incidents is as below –

| Type of information security incidents | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|
| Cyber attack compromising information systems | 1 | 1 | – | 1 | – | – |
| Abuse of information systems or operational faults | – | 2 | 1 | 2 | 1 | – |
| Loss or theft of mobile devices or removable media | 1 | 1 | 4 | 2 | 1 | 1 |
| Totali¼š | 2 | 4 | 5 | 5 | 2 | 1 |

In accordance with the prevailing guidelines, the data involved in the above incidents had been backed up and duly encrypted. The operation of the departments was not affected.

The government has established a set of response mechanism and measures to deal with information security incidents and requires all departments to follow strictly. According to this requirement, when a security incident has occurred, the concerned department must report it to the Government Information Security Incident Response Office, submit an incident report and promptly conduct an investigation as well as rectify the problem. For those incidents involving personal data, we have also reported to the Office of the Privacy Commissioner for Personal Data, notified all affected persons and provided them with the appropriate advice on information security. If criminal conduct may be involved, the relevant department must report such incidents to the police for investigation. In addition, public officers must strictly follow the relevant regulations, including the Official Secrets Ordinance, the Security Regulations and the Civil Service Code.

The OGCIO will review and update the prevailing Policy and Guidelines from time to time. In August 2019, OGCIO launched a new round of review and update which is expected to be completed within this year. The review will continue to make reference to the latest international standards and industry best practices, and examine and update the existing Policy and Guidelines in the light of latest developments in information and cyber security, so as to safeguard government information systems and data security more effectively.