LCQ18: Cybersecurity of government departments and other public organisations

Following is a question by the Hon Chan Hak-kan and a written reply by the Secretary for Innovation, Technology and Industry, Professor Sun Dong, in the Legislative Council today (May 29):

Question:

It has been reported that cybersecurity incidents, including unauthorised access into computer systems by hackers and leakage of personal data, have occurred one after another in government departments and other public organisations in recent years, which have aroused public concern and worries. In this connection, will the Government inform this Council:

(1) whether it has compiled statistics on the number of data leakage incidents that occurred in government departments and other public organisations in the past three years; of the follow-up actions taken by the government departments in respect of such incidents, including whether they have imposed penalties on the responsible personnel concerned, and whether the law enforcement agencies concerned have investigated if such incidents involved criminal elements; if the government departments and law enforcement agencies have, of the details; if not, the reasons for that;

(2) of the mechanism in place to ensure and monitor compliance by government departments and other public organisations with the Guidance Note on Data Security Measures for Information and Communications Technology drawn up by the Office of the Privacy Commissioner for Personal Data, Hong Kong;

(3) given that according to the Baseline IT Security Policy formulated by the Office of the Government Chief Information Officer, civil servants who contravene the IT security policy may be subjected to relevant disciplinary actions, whether any civil servant has been subjected to disciplinary actions as a result of the data leakage incidents mentioned in (1); if so, of the details; if not, the reasons for that;

(4) whether it has compiled statistics on the number of local cybersecurity-related professionals, and of the measures in place to train more relevant professionals, so as to enhance the cybersecurity of government departments and other public organisations; and

(5) of the specific plans and measures (including amending or enacting the relevant legislation) the Government has in place in the coming year to enhance the cybersecurity of government departments and other public organisations?

Reply:

President,

Regarding the Hon Chan Hak-kan's question, in consultation with the Constitutional and Mainland Affairs Bureau, the Civil Service Bureau (CSB), the Security Bureau and the Labour and Welfare Bureau, the reply is as follows:

(1) and (3) Under the existing Government Information Technology Security Policy and Guidelines, when an information technology (IT) security incident occurred, the concerned bureaux and departments (B/Ds) must report it to the Government Information Security Incident Response Office, and notify as appropriate the Office of the Privacy Commissioner for Personal Data (PCPD) and/or the Police depending on the nature of incident. In the past three years, the Office of the Government Chief Information Officer (OGCIO) received a total of seven information security incident reports that might involve data leakage of individual government departments. We do not maintain any information regarding information security incidents of public organisations.

B/Ds responsible for the IT systems related to the above incidents will set up task force to conduct comprehensive investigation of the causes of individual incident. The heads of B/Ds will handle cases in accordance with the established procedure if their personnel or contracted service providers are suspected of violating relevant regulations or engaging in illegal acts. The CSB does not comment on the disciplinary cases of individual officers.

(2) Government B/Ds must comply with the requirements set out in the Policy and Guidelines. The relevant information security principles are generally in line with the directions of the measures recommended in the Guidance Note on Data Security Measures for Information and Communications Technology issued by the PCPD, covering for example encryption of data during transmission and storage, prohibition against storing sensitive and personal data on public cloud platforms, and conducting regular security risk assessment and audits (SRAA) by B/Ds for their IT infrastructure, information systems and data assets. The Policy and Guidelines is also published for reference by the industry (including both public and private organisations) and their formulation of appropriate IT security measures having regard to their own situations.

(4) According to the manpower survey conducted by the Vocational Training Council in 2022, the number of IT security-related professionals in Hong Kong was 1 587, about half of whom were cyber security-related professionals. The Government is carrying out a new round of Manpower Projections to gauge the manpower requirements for major industries (including the innovation and technology industry) in the coming five years. Key findings are expected to be available in the third quarter of this year and a full report will be released in early 2025 at the earliest. This would help facilitate our human resources planning related to cyber security.

The OGCIO is committed to promoting various initiatives to facilitate the comprehensive development of the IT security industry in Hong Kong, nurture manpower and strengthen the cyber security defence capability of

relevant personnel. These initiatives include:

(i) collaboration with the IT industry to regularly organise activities such as thematic seminars, technical workshop, certificate courses on information security, cyber security incident response training and the Information Security Summit, so as to enhance IT practitioners' information security skills and knowledge;

(ii) working in partnership with the industry to hold different promotion activities such as school visits, InfoSec Tours, the Cyber Youth Programme and the Hong Kong Cyber Security New Generation Capture the Flag Challenge, to enhance youngsters and students' knowledge and interest in cyber security, thereby encouraging and grooming more talents for the information security industry; and

(iii) supporting tertiary institutions in their provision of more information security programmes, collaboration with professional information security associations to promote professional accreditation for IT practitioners, and organising activities including seminars and workshops which aim to nurture more IT practitioners with information security knowledge and skills.

(5) To ensure the smooth implementation and operation of government IT systems, the OGCIO introduced a series of new measures to B/Ds in February 2024, including arranging additional independent cyber security tests such as simulated real-world intrusion attack drills for large-scale and high-risk IT projects before launch, which help B/Ds to detect and patch relevant systems' vulnerabilities at an early stage and assess the detection and resilience capabilities of the systems in response to cyber attacks. The OGCIO is also actively examining measures on enhancing B/Ds' usual SRAA for information systems, regular network monitoring, spot checks, compliance audits and staff training, so as to strengthen the abilities to monitor and safeguard for government information systems.

In addition, the OGCIO will take the lead in organising cyber security attack and defence drills in the second half of this year to test and strengthen the information systems security of government departments and public bodies, by leveraging the capabilities and experiences of Mainland organisations specialised in attack and defence drills. The OGCIO will also continue to update the Policy and Guidelines from time to time with reference to the latest technological development as well as national and international information security management standards, with a view to strengthening the Government's IT security requirements and addressing the increasing cyber security risks.

To enhance the protection of cyber security of critical infrastructures, the Government plans to define clearly, through legislation, the cyber security 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 Security Bureau aims to introduce a Bill into the Legislative Council within this year.