LCQ11: Cybersecurity of government departments and other public organisations

Following is a question by the Hon Edward Leung and a written reply by the Secretary for Innovation, Technology and Industry, Professor Sun Dong, in the Legislative Council today (November 22):

Question:

It is learnt that as the Government is promoting the development of Hong Kong into a smart city and as more public organisations are implementing electronic services, the public has expressed increasing concerns on the cybersecurity measures they adopt. In this connection, will the Government inform this Council:

(1) in relation to the recent cyberattacks on the Cyberport and the Consumer Council, whether the Government knows the major root causes leading to the data breaches and why such root causes were not found in previous security assessments;

(2) of the number of systems (such as websites, apps and hosts) of government departments and other public organisations which were attacked by ransomware last year, and the number of such attacks not disclosed to the public;

(3) of the number of systems mentioned in (2) which were covered by continuous security assessment and improvement programs (such as vulnerability disclosure program and bug bounty program); and

(4) whether it has estimated the talent gap of cybersecurity talents required to be filled to address the needs of government departments and other public organisations for continuous security assessments and improvements?

Reply:

President,

The Government is very 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.

Having consulted the Commerce and Economic Development Bureau and the Security Bureau, my reply to the questions raised by the Hon Edward Leung is as follows:

(1) The cybersecurity incident at Cyberport in August 2023 was caused by ransomware. As soon as its computer systems were suspected of being intruded

by hackers, Cyberport had implemented multiple measures immediately, including strengthening cybersecurity and system's defence, engaging independent cybersecurity expers for investigation and review, and reporting the case to the Police and the Office of the Privacy Commissioner for Personal Data (PCPD). Cyberport had also made public announcements on the incident and the latest development, and notified the known potentially affected persons to offer them assistance as far as possible. In this connection, the Board of Directors of Cyberport had established a Task Force to monitor the relevant follow-up actions.

Meanwhile, the computer system of the Consumer Council (the Council) was similarly attacked by hackers with ransomware in end-September 2023. Upon discovering the intrusion, the Council had immediately taken multiple follow-up actions, including strengthening security measures of the system, reporting to the Police and PCPD, and appointing a forensic expert to conduct investigations. The Council had also held a press briefing to inform the public of the incident and contacted the potentially affected persons to urge them to stay vigilant and suggest measures to be taken, including avoiding opening or clicking on suspicious links, emails or messages.

(2) and (3) With regards to the security of information systems and cyberspace, the Government has devised and implemented on an ongoing basis a multi-layered system covering assessment, monitoring, risk management and contingency. To ensure the safety of government information systems, all government departments must adopt a risk-based approach to continuously identify security risks of their information systems by regularly conducting independent information security risk assessments and reviewing and enhancing current security measures to keep relevant measures abreast of the times and ensure their effectiveness in tackling the latest cyber risks. On the other hand, in view of evolving pattern of cyber attacks, the Office of the Government Chief Information Officer (OGCIO) has been closely monitoring the trends of cyberattacks and the associated security threats, and issued timely security alerts and reminders to government departments to assist and remind them of their obligation to make prompt responses and strengthen their precautionary measures.

Besides, the Critical Infrastructure Security Coordination Centre (CISCC) of the Police is committed to strengthening the protection and resilience of critical infrastructure through public-private partnership, risk management and on-site security inspections, etc. By instilling the concept of Security-by-Design and providing professional security recommendations, the CISCC seeks to enhance critical infrastructure's capacity in defence, response and recovery. Meanwhile, the Cyber Security Centre under the Cyber Security and Technology Crime Bureau (CSTCB) of the Police provides round-the-clock cyber security protection and conduct timely cyber threat audits and analyses for critical infrastructure in the sectors of government, banking and finance, transportation, communications and public utilities, so as to prevent and detect cyberattacks against critical infrastructure.

The Government's information security incident response mechanism requires all government departments to report information security incidents to the OGCIO when such security incident occurs. Last year, the OGCIO received in total five information security incident reports on ransomware infection of government information systems, which did not involve information leakage. Figures of the afore-mentioned information security incidents have been published in the Data.Gov.HK portal. The Government does not maintain statistics of cyberattacks on public organisations.

(4) Cybersecurity concerns various segments of information technology (IT), and hence the Government did not make any estimation on the demand and supply of the cybersecurity-related manpower. To promote the comprehensive development of IT security industry and grooming of talents, as well as to strengthen capability of relevant practitioners on cybersecurity protection, the Government has been promoting the following measures:

(i) The OGCIO and the IT industry regularly organise activities including thematic seminars, technology workshop, certificate courses on information security, cybersecurity incident response training and the Information Security Summit to enhance IT practitioners' skills and knowledge of information security;

(ii) The OGCIO collaborates with the industry on holding different promotion activities such as school visits, InfoSec Tours, Cyber Youth Programme, Hong Kong Cyber Security New Generation Capture The Flag Challenge, etc. to enhance the knowledge and interest in cybersecurity amongst young people and students, thereby encouraging and grooming more talents for the information security industry;

(iii) The OGCIO supports tertiary institutions to provide more information security programmes, works with professional information security associations to promote professional accreditation for IT practitioners and holds activities including seminars and workshops, which aim to equip more IT practitioners with information security knowledge and skills;

(iv) The Government seeks to attract technology talents from all over the world through the Technology Talent Admission Scheme to work in the research and development fields including information security industry in Hong Kong, so as to enrich Hong Kong's pool of talents on information security; and

(v) The CSTCB has established the Cyber Range, which provides a safe and controlled virtual environment for training police officers and other cyber security practitioners under simulated cyberattack and defence scenarios, thereby helping to develop professional competence of stakeholders in order to strengthen the safeguard of cybersecurity in Hong Kong.