LCQ7: Information security of government departments and public organisations

Following is a question by the Hon Jeffrey Lam and a written reply by the Secretary for Innovation, Technology and Industry, Professor Sun Dong, in the Legislative Council today (March 26):

Question:

Last month, an information security incident occurred in Invest Hong Kong (InvestHK) in which its computer systems were attacked by malicious ransomware, affecting its internal Customer Relationship Management system, intranet, website operations, etc. Regarding the occurrence of cybersecurity incidents in government departments and public organisations, will the Government inform this Council:

(1) of the following information on malicious ransomware attacks on government departments and public organisations in the past three years: (i) the number of cases, (ii) the government departments and public organisations involved, (iii) the number of cases involving leakage of personal, customer or internal data, and (iv) the number of culprits arrested in connection with such cases;

(2) given that Hong Kong is actively attracting businesses and talents, whether the Government has received public complaints or enquiries about the aforesaid information security incident of InvestHK; if so, of the number; whether the Government has assessed if the information security incident has dampened investors' confidence in the information security of InvestHK, or even investors' interest in investing in Hong Kong; and

(3) of the measures the Government has put in place to strengthen the security of the computer and information systems of government departments and public organisations, and the expected time for conducting a review of the effectiveness of such measures, so as to continuously ensure the security of the relevant systems of such departments and organisations?

Reply:

President,

In respect of the question raised by the Hon Jeffrey Lam, having consolidated the information provided by the Security Bureau and the Commerce and Economic Development Bureau, my reply is as follows:

(1) According to the Government Information Technology Security Policy and Guidelines, when an information technology (IT) security incident occurs, the concerned bureaux and departments (B/Ds) must report it to the Government Information Security Incident Response Office under the Digital Policy Office

(DPO), and notify the Office of the Privacy Commissioner for Personal Data (PCPD) and/or the Police depending on the nature of the incident.

In 2022, 2023 and 2024, the DPO received 5, 3 and 2 incident reports respectively that involved ransomware attack of government IT systems. None of these incidents resulted in any data leakage. In view of the nature of the incidents, the sensitivity of the information and security considerations, the departments concerned considered it as inappropriate to publish relevant details, in order not to increase the risk of malicious intrusion into government systems. Upon receipt of the incident reports, the DPO had promptly assisted relevant departments in handling the incidents and provided technical advice to enhance their information security.

As for public bodies, neither the DPO nor the Hong Kong Computer Emergency Response Team Coordination Centre has received any notification of information security incidents from public bodies relating to ransomware attack in the past three years. However, we note that individual public bodies have taken the initiative to make public announcement on relevant incidents having regard to the nature and specific circumstances of the case. To enhance the information security of public bodies and strengthen the incident handling mechanism, the Government has since August 2024 required public bodies to notify the relevant B/Ds of incidents relating to their designated IT systems. As at mid-March this year, the Government has not received any relevant report.

Depending on the circumstances of the case, there is a possibility that a ransomware attack may constitute a breach of "criminal intimidation" (section 24 of the Crimes Ordinance), "criminal damage" (section 60 of the Crimes Ordinance), "access to computers with criminal or dishonest intent" (section 161 of the Crimes Ordinance), or other related offences. The Police does not maintain breakdown statistics on the number of arrests for ransomware attacks.

(2) On February 22 this year, Invest Hong Kong (InvestHK) identified an information security incident which involved a malicious ransomware attack to part of InvestHK's computer systems. Upon identification of the incident, the Department took immediate measures to tighten security of its IT systems to prevent further ransomware attacks. In line with the established procedures, it has on the same day also reported the case to the Police, the DPO, the PCPD and the Security Bureau respectively. According to InvestHK's investigation findings, there was no evidence indicating leakage of personal information. No further suspicious activities have been identified since then. As at mid-March this year, the Department has not received any public complaints or enquiries related to this information security incident. After the incident, InvestHK promptly issued press releases to clearly explain the situation to the public and its clients. It is believed that the incident has not affected investors' confidence. InvestHK has all along been observing the Government's procedures in its information and cybersecurity work. It will continue to cooperate with the DPO and adopt experts' recommendations in tightening its IT security systems, so as to prevent similar incidents from happening again.

(3) To enhance the IT security of B/Ds and public bodies, the Government has implemented several enhancement measures which require B/Ds and public bodies under their purview to strengthen the project governance and security of IT systems, including key initiatives such as:

(i) Strengthen oversight responsibility: all B/Ds must appoint a senior directorate officer or the head/ deputy head of the management team of relevant organisation to oversee information security work, and immediately assess and strengthen their existing cybersecurity measures, in order to guard against cyberattacks.
(ii) Regular tests, assessments and audits: all B/Ds and public bodies must arrange additional stress tests and security tests by an independent third party before rollout of their IT systems, and perform security risk assessments for their IT systems at least once every two years. Security risk assessments shall identify and determine the level of IT security risks of an IT system based on risk sources (e.g. vulnerabilities, threats), events (e.g. incident scenarios), and risk impact and likelihood, so as to help prioritise the identified risks for risk management and updating of response measures.
(iii) System health check, penetration test and compliance audit: the DPO introduced a centralised cybersecurity health check platform to conduct regular and continuous health checks and penetration testing on the government's public-facing IT systems to enhance B/Ds' ability to identify potential security vulnerabilities, thereby strengthening the prevention of information and cybersecurity incidents. The DPO also launched a new round of government-wide information security compliance audit in 2024, and will select eight government IT systems for in-depth information security compliance audit in 2025.
(iv) Real-life cybersecurity attack and defence drills: starting from 2024, the DPO will organise annual real-life cybersecurity attack and defence drill, and invite different B/Ds and public bodies to participate. The drills will simulate real-life cyberattacks to test the response and resilience of IT systems in the event of cyberattacks, with a view to enhancing the technique, experience and overall defence capabilities of B/Ds and public bodies through the drills and fortifying the defence line.
(v) Step up staff training: the DPO and the Civil Service College jointly organise thematic seminars under the Innovation and Technology leadership series for the senior management of all B/Ds, and provide latest cybersecurity trends and preventive measures to enhance their information security knowledge.