LCQ12: Cyber security risks amid the epidemic

Following is a question by the Hon Martin Liao and a written reply by the Secretary for Innovation and Technology, Mr Alfred Sit, in the Legislative Council today (May 26):

Question:

It has been reported that amid the Coronavirus Disease 2019 epidemic which rages across the globe, the computer systems of hospitals in quite a number of places and even the World Health Organization have been subjected to intensified attacks by hackers. The number of cyberattacks such as phishing emails that the Hospital Authority (HA) of Hong Kong was subjected to surged from about 20 million in 2015 to over 50 million last year. Besides, the HA was also subjected to five ransomware email attacks last year. An international cyber security analysis report pointed out that last year amid the epidemic, the industries most targeted by cyberattacks, apart from health care industry, were business and professional services industries, retail and hospitality industries, financial industry and high technology industry. In this connection, will the Government inform this Council:

(1) whether it knows the number of cyberattacks that Hong Kong's health care industry was subjected to in each of the past three years, and the annual rates of change of such numbers, with a breakdown of such cases by type of institutions/organisations and type of attacks, as well as the losses involved (if any);

(2) whether it knows the number of cyberattacks that other industries in Hong Kong were subjected to in each of the past three years, and the annual rates of change of such numbers, with a breakdown of such cases by industry and type of attacks, as well as the losses involved (if any);

(3) whether it has assessed the cyber security risks faced by the various industries in Hong Kong amid the epidemic; if so, of the details; if not, the reasons for that; and

(4) whether it knows the new trends and major concerns in respect of cyber security risks across the globe amid the epidemic; if so, of the details and their impacts on Hong Kong?

Reply:

President,

Regarding the various parts of the question, our consolidated reply is as follows:

In the past year or so, COVID-19 has been rampant across the globe, and has significantly changed enterprises' mode of operation and people's way of living. Remote business, work from home, remote learning and online shopping etc. have become the new normal. Under this new normal, various sectors have to undergo digital transformation on the one hand, and on the other hand, actively respond to the new cyber security risks brought about by the transformation.

The breakdown of statistics on information security incidents handled by the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) over the past three years is at Annex I. According to the statistics, a total of 8 346 information security incidents were handled in 2020, representing a decrease of 17 per cent and 12 per cent as compared with 2018 and 2019 respectively. Although there was a downward trend in the overall number of incidents, the phishing cases increased to 3 483, representing an increase of 66 per cent and 35 per cent as compared with 2018 and 2019 respectively. We note that many hackers took advantage of the public concern over the epidemic by disseminating false information through phishing methods or pretending to be health organisations seeking donations, so as to lure the victims into visiting malicious websites, disclosing sensitive information or even defrauding money. In addition, the number of malicious software cases (mainly targeting individuals) in 2020 fell sharply by 85 per cent to 181 cases as compared with that in 2019. There were signs indicating that hackers have switched their main targets to enterprises or organisations. On the other hand, despite the small number of distributed denial-of-service (DDoS) attacks at 53 cases only, the increase was over 43 per cent when compared with that in 2019. Such increase was believed to be due to the increase in the "attack surfaces" resulting from the provision of more online services by various sectors during the epidemic.

Besides, the Hong Kong Police Force (HKPF) recorded a total of 12 916 technology crime cases in 2020, representing an increase of 55 per cent as compared with 8 322 cases in 2019. The average monetary loss per case decreased from about $350,000 in 2019 to about $230,000, and the total amount of monetary loss was about $2.96 billion, similar to that in 2019. The rise in the number of technology crime cases was mainly due to the increase in online fraud (such as e-shopping fraud or romance scam). Fraudsters commit offences with technologies such as the Internet, social media and e-mail as the medium. The breakdown of technology crimes and related loss over the past three years is at Annex II. The HKCERT and the HKPF do not have information on the breakdown by enterprise, organisation and industry (including the healthcare sector).

The Government has all along been maintaining close collaboration with the HKCERT to closely monitor the impact of the epidemic on global and local cyber security risks. Under the epidemic, the HKCERT expects a proliferation of targeted and organised cyberattacks on a global scale, which aligns with the local cyber security trend. Enterprises must be well-prepared to cope with the related challenges.

We will continue to tackle information security issues through a multi-

pronged strategy. For example, by providing financial subsidy (such as Technology Voucher Programme), we support enterprises to enhance systems and cyber security measures, so as to strengthen the level of information security of various sectors. We also work closely with the Hong Kong Internet Registration Corporation Limited and the HKCERT to disseminate information and advice on cyber security matters to the public. In addition, we encourage more public and private organisations' exchange of cyber security information through the Partnership Programme for Cyber Security Information Sharing and the cross-sector Cyber Security Information Sharing and Collaborative Platform (Cybersechub.hk). Moreover, the HKCERT has been implementing the Healthcare Cyber Security Watch Programme since 2019 to notify Hong Kong healthcare sector of cyber security vulnerabilities and threats in order to reduce cyber security risks. We will continue to collaborate with relevant organisations and departments (such as the HKPF and the Office of the Privacy Commissioner for Personal Data) to enhance Hong Kong's overall defense capability and resilience against cyberattacks, and strive to build Hong Kong as a safe and secure smart city.