For discussion
on 10 May 2021

Legislative Council
Panel on Information Technology and Broadcasting

Update on Information Security

Purpose

This paper briefs Members on the latest situation of information security in Hong Kong and the Government's work on information security in the past year.

Background

2. Innovation and technology plays a key part in stimulating economic development. It does not only give impetus to social advancement, but also enhances people's quality of life. In the past year, 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". With the wider application of information technology (IT), the threat of cyber attacks should not be overlooked. In this regard, the Government, enterprises and members of the public have to raise their awareness of cyber security in order to continuously improve the defence and response capability of our society as a whole.

Overall Situation of Information and Cyber Security

3. Under the "new normal", enterprises have to undergo digital transformation on the one hand, and on the other hand actively respond to the information security challenges brought about by the transformation. The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) handled a total of 8 346 security incidents in 2020, representing a drop of 12% from 9 458 cases in 2019. The main categories of information security incidents were botnets (4 154 cases) and phishing

(3 483 cases). The number of botnets cases decreased by 16% when compared with that in 2019, while the number of phishing cases increased by 35% when compared with that in 2019, which was by and large consistent with the global cyber security trend. Phishing mainly took advantage of the public's concern over the epidemic and by disseminating false information or purporting to be health organisations seeking donations. Victims were lured into visiting malicious websites or disclosing sensitive information, or even defrauded them of their money. Besides, the number of malicious software (including ransomware) cases fell sharply by 85% to 181 cases, as attackers switched their main target to enterprises, resulting in a significant decrease in the number of malware incidents targeting at individuals. In addition, despite the small number of distributed denial-of-service (DDoS) attacks at 53 cases only, the increase was over 43% 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. In the first quarter of 2021, HKCERT handled a total of 2 004 security incidents, of which phishing (988 cases) and botnets (864 cases) were still the main categories. The breakdown of statistics on security incidents is at **Annex I**.

4. The Hong Kong Police Force (HKPF) recorded a total of 12 916 technology crime cases in 2020, representing an increase of 55% 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 through technologies such as the Internet, social media and e-mail as the medium. In the first two months of 2021, HKPF recorded a total of 2 158 technology crime cases and the monetary loss was about $5 million. The breakdown of the technology crimes is at **Annex II**.

Information Security Measures in the Community

5. The Government is committed to providing the community with a secure and reliable cyber environment, including enhancing the awareness and response capability of public and private organisations as well as members of the public on cyber security, and nurturing cyber security

professionals. The Office of the Government Chief Information Officer (OGCIO), HKCERT, the Cyber Security and Technology Crime Bureau of HKPF, and the Hong Kong Internet Registration Corporation Limited (HKIRC) have all along been working closely to provide appropriate support to the public.

(I) *Enhancing the capability of Hong Kong enterprises (including small and medium enterprises (SMEs)) in responding to various cyber attacks*

Monitoring and responding to cyber threats and attacks

6. HKCERT has all along been providing computer security information to the Internet community in Hong Kong. From 2020 to the first quarter of 2021, HKCERT issued more than 450 cyber security information and security recommendation to industries and the public, and organised seminars and competitions to promote best information security practices and raise public awareness of cyber security.

7. Given the importance of cyber security to individual industries, HKCERT joins hands with several industries' chamber of commerce to organise thematic seminars to further promote cyber security awareness among the industry. From 2020 to the first quarter of 2021, HKCERT organised more than 25 seminars, attracting over 3 200 practitioners from various sectors, including financial services, insurance, industry, education, retail, catering and IT etc. HKCERT will continue to cooperate with various industries' chamber of commerce to promote the importance of cyber security, and support individual sectors to implement security measures.

Cyber security preventive service and information sharing

8. To assist local SMEs with limited resources in coping with the increasingly complicated cyber security threats, the Government joined hands with HKIRC in mid-2019 to launch a free scanning service for SME's websites, including checking whether the websites have security vulnerabilities, conducting briefings on scanning reports and providing mitigation solutions to assist SMEs in identifying potential security vulnerabilities as early as possible. As of the first quarter of 2021, HKIRC has provided scanning services to about 2 000 local SMEs.

9. Moreover, OGCIO regularised the cross-sector "Partnership Programme for Cyber Security Information Sharing" (Partnership Programme) in September 2020 and partnered with HKIRC to support its operation to promote more public and private organisations (in particular SMEs) in exchanging cyber security information. So far, over 420 public and private organisations have joined the programme, covering a wide range of sectors, including finance and insurance, public utilities, transport, medical care, telecommunications, innovation and technology, information security and tertiary education institutions etc. With regards to the financial sector, under the support of the Hong Kong Association of Banks, more than 120 banks have participated in the programme. The Partnership Programme has a collaborative platform for participating members to exchange information on cyber security threats, mitigation measures and best practices etc. Members of the public can also obtain security alerts and advice from experts in the public zone of the platform. The Partnership Programme actively enhances exchanges in key industries (such as banking and medical care sectors etc.), organises sector-specific seminars and sets up individual groups on the collaboration platform for information sharing.

10. The platform will acquire cyber security threat intelligence from more varied channels (including free open source and paid commercial source) later this year, and will add Application Programming Interfaces to facilitate the automatic exchange of cyber threat information among different information security systems to enable participating members to defend against cyber attacks more rapidly. We will continue to strengthen promotion, encourage more organisations from different sectors to join the Partnership Programme, and actively promote the sharing of cyber security information.

(II) *Responding to information security challenges under the epidemic*

11. The Government has been providing financial support to strengthen the level of information security of enterprises, including the Technology Voucher Programme (TVP) which subsidises local non-listed enterprises and organisations in using technological services and solutions to improve productivity or upgrade and transform their business processes. Enterprises can utilise the funding to enhance systems and cyber security measures, including defending against cyber attacks and implementing disaster recovery solutions. In April 2020, the Government further enhanced the TVP by raising the matching ratio for each funded project to

3:1, increasing the funding ceiling for each enterprise to $600,000 and the maximum number of approved projects to six. Since 2016, TVP has funded more than 330 projects related to the upgrading of information systems and cyber security. The relevant funding amount is about $45 million.

12. The Government launched the Distance Business Programme (D-Biz Programme) under the Anti-epidemic Fund to subsidise enterprises to use IT solutions for developing remote business to support enterprises to continue operation during the epidemic. The programme covers 12 IT solution categories related to remote business, which also include cyber security solutions to strengthen defence against cyber attack and enhance the security of information systems of enterprises. The D-Biz Programme has approved more than 3 000 IT solutions related to cyber security, involving a funding amount of around $82 million.

13. In 2020, HKCERT also provided appropriate security advice and guidelines from time to time to assist enterprises and the public in using online service securely, such as educational videos on the security of online meetings and security guidelines for remote access and Virtual Private Network of enterprises. HKCERT also closely monitored the relevant cyber attacks in specific sectors (such as medical care and logistics sectors etc.) in order to provide enterprises with information on security threats in a timely manner, such as reminding enterprises to watch out for phishing and DDoS attacks etc. and implement corresponding defensive measures. The Office of the Privacy Commissioner for Personal Data (PCPD) also published practical guidance notes relating to work-from-home arrangements to provide advice to users of video conferencing service to enhance information security and protection of personal data privacy. HKPF continued to strengthen publicity and education in raising the public awareness of fraud prevention to avoid falling into cyber pitfalls. In 2021, HKPF has included the strengthening of cyber security and combating technology crime as one of their top operational priorities. They will continue to combat and prevent various types of fraud to minimise the loss of victims through the Anti-Deception Coordination Centre.

(III) <u>Public education</u>

14. In view of the increasing use of mobile devices in Hong Kong, OGCIO, HKPF and HKCERT organised a series of promotional activities in 2020 with the theme "Secure Use of Mobile Devices" to arouse public

awareness of information security related to mobile devices. OGCIO also worked with HKCERT to produce a series of cyber security animation videos which are interesting and easy to understand for promotion to the public and SMEs through social media. In view of the recent personal data breach incidents relating to users of social media platforms from time to time, HKCERT and PCPD issued security blogs and guidelines respectively to remind the public of the security and privacy risks of using social media and instant messaging software. Practical advice on mitigation of risks and protection of personal data privacy was also provided.

15. Moreover, OGCIO and HKIRC jointly organised the "Security and Law in Cyber World" webinar in March 2021. Apart from enhancing cyber security knowledge of participants, the webinar also reminded them that the cyber world was also governed by existing laws to strengthen their law-abiding awareness when conducting online activities.

16. In the two school years of 2019/20 and 2020/21 (as at the first quarter of 2021), OGCIO and professional bodies jointly organised more than 20 physical or virtual school visits, conveying information security messages to more than 5 100 teachers and students. Besides, as the use of IT has gained popularity among the elderly, OGCIO has conducted cyber security talks for elderly service centres either physically or virtually to enhance their security awareness.

17. In 2020, OGCIO enhanced the one-stop information security portal "InfoSec" to facilitate more convenient retrieval of various information related to information security by the public. The website is categorised according to different themes for easy browsing by different people. OGCIO will continue to collaborate with different organisations and extend the reach through various channels, including websites, social media, text media, etc., to strengthen the dissemination of different types of cyber security information to the public.

(IV) *Supporting national security education*

18. In April 2021, OGCIO collaborated with HKPF to provide information related to cyber security for the public education exhibition on the "National Security Education Day" to strengthen the public's understanding of the importance of cyber security to national security. To tie in with the "China Cybersecurity Week" to be held in September,

OGCIO will continue to organise the annual "Build a Secure Cyberspace" promotional campaign in conjunction with HKPF and HKCERT to strengthen organisations' and the public's understanding of cyber security and national security, and remind them to behave prudently in the cyber world, jointly maintain cyber security and avoid falling into cyber pitfalls or even breaching the law inadvertently.

Manpower Development in Information Security

19. In January 2021, the Government enhanced the Technology Talent Admission Scheme (TechTAS) and extended its coverage to all companies in Hong Kong conducting research and development activities in the designated technology areas (including cyber security). This is to enable more companies to benefit from the scheme and the streamlined procedures, thus expediting the admission of cyber security technology talents to Hong Kong from different parts of the world.

20. In November 2020, the Hong Kong Productivity Council and HKCERT jointly organised the first "Hong Kong Cyber Security New Generation Capture the Flag Challenge 2020" to nurture more talents aspiring to a career in cyber security industry and increase the interest of local tertiary and secondary school students in cyber security. The school sector has responded enthusiastically with a total of 156 teams with nearly 540 students from 37 secondary schools and 19 tertiary institutions participated. The competition will continue to be held in 2021.

Internal Measures to Tackle Cyber Security Threats in the Government

(I) *Review of Government IT security policy*

21. In the face of rapid technological development and emerging security threats, OGCIO completed the comprehensive review of the "Government IT Security Policy and Guidelines" in March 2021 and promulgated the revised and updated version. The review made reference to the latest international standards and industry's best practices, and strengthened the requirements in specific security domains, such as making reference to "ISO 27701 Privacy Information Management" to enhance the management requirement of personal data protection, strengthening the risk

management of Internet of Things and public cloud services, and enhancing the requirements for information systems such as software management and testing. In response to departments' needs under the work-from-home arrangement during the epidemic, the revised and updated version also strengthens the protection of remote access to departmental network and information systems. The latest "Government IT Security Policy and Guidelines" has been uploaded to the website of OGCIO for public reference.

(II) *Promoting security of smart city infrastructure*

22. The Government released the "Hong Kong Smart City Blueprint 2.0" in 2020 which endeavours to improve the quality of life of the people and assist in fighting against the epidemic through wider use of technology, for example, the "iAM Smart" platform, the "StayHomeSafe" quarantine system, the "LeaveHomeSafe" exposure notification system, the new generation government cloud infrastructure and the big data analytics platform etc. In the development of relevant systems and infrastructure, the Government has strictly followed the requirements of the "Government IT Security Policy and Guidelines" and the "Personal Data (Privacy) Ordinance", and has engaged independent third parties to conduct privacy impact assessments as well as information security risk assessments and audits at different implementation stages of the project to ensure that the security of systems and data and privacy of the public are properly safeguarded.

(III) *Information sharing and threat alerts*

23. In the past year, OGCIO utilised big data analytics to collect and analyse cyber threat information from different sources, conduct collation and evaluation, strengthen its capability to issue cyber threats and early warning, and remind bureaux and departments (B/Ds) to fix security vulnerabilities as soon as possible. From 2020 to the first quarter of 2021, OGCIO issued over 120 security alerts in relation to computer system or software vulnerabilities, and required all B/Ds to take appropriate preventive measures promptly to ensure the security of Government information systems and data assets.

(IV) *Staff training and technical support*

24. In January 2021, OGCIO organised the fifth "Inter-departmental Cyber Security Drill" jointly with HKPF. Through drills and workshops simulating multiple cyber attack scenarios, government officials acquired an understanding of cyber attacks and practical incident handling procedures in relation to remote work so as to improve B/Ds' capability to defend against and respond to cyber security incidents.

25. In 2020, OGCIO organised a number of webinars and solution showcases to enhance the information security knowledge of government officials. From 2020 to the first quarter of 2021, around 2 000 government officials took part in these events to learn about the latest cyber security trends and information security preventive measures for work-from-home arrangement. OGCIO also organised the "Government-wide Phishing Drill Campaign" and encouraged staff to pursue internationally recognised information security certificates in order to consolidate and strengthen their professional knowledge.

26. OGCIO continues to enhance the functions of the network cum system testing platform to assist B/Ds in conducting security and penetration testing for their online systems and websites in order to identify potential vulnerabilities and fix them as early as possible. From 2020 to the first quarter of 2021, the testing platform provided timely and convenient security testing service to more than 830 government websites and various epidemic-related emergency systems.

(V) *Compliance audits*

27. In order to tackle emerging information security threats, OGCIO regularly conducts independent information security compliance audits for B/Ds to ensure that they strictly comply with the security requirements of the Government, and offers advices to assist them in continuously improving their security management systems. The compliance audit report will be submitted directly to the heads of departments for reference and follow-up. As of the first quarter of 2021, OGCIO completed a new round of audits for 21 B/Ds. It is expected that the audits for all B/Ds will be completed in the first quarter of 2022.

Way Forward

28. Apart from maintaining cooperation with enterprises and organisations from various sectors to enhance cyber security awareness and capabilities in the community, the Government will continue to strengthen the nurturing of local cyber security talents, promote best practices in information security, enhance cyber security of enterprises through different measures, as well as cooperate and share information security intelligence internationally and with the Mainland to build Hong Kong into a safe and secure smart city.

Advice Sought

29. Members are invited to note the contents of the paper.

Innovation and Technology Bureau
Office of the Government Chief Information Officer
May 2021

Annex I

Breakdown of Statistics on Security Incidents Handled by The Hong Kong Computer Emergency Response Team Coordination Centre

Incident Category	2019		2020			2021 (As at March)	
	Number of cases	**%**	**Number of cases**	**%**	**Compared with 2019 (%)**	**Number of cases**	**%**
Botnet	4 922	*52*	4 154	*50*	*-16*	864	*43*
Phishing (including phishing emails and websites)	2 587	*27*	3 483	*42*	*+35*	988	*49*
Malicious Software (including ransomware)	1 219	*13*	181	*2*	*-85*	23	*1*
Distributed Denial-of-Service (DDoS) Attacks	37	*<1*	53	*<1*	*+43*	5	*<1*
Hacker Intrusion/Web Defacement	48	*<1*	36	*<1*	*-25*	4	*<1*
Others[1]	645	*7*	439	*5*	*-32*	120	*6*
Total:	**9 458**	***100***	**8 346**	***100***	***-12***	**2 004**	***100***

[1] Including identity theft, data leakage, etc.

Annex II

Statistics on Technology-related Crimes Handled by the Hong Kong Policy Force and the Monetary Loss

	2019	2020		2021 (As at February)
Case Nature	**Number of cases**	**Number of cases**	**Compared with 2019 (%)**	**Number of cases**
Internet Deception	5 157	10 716	*+108*	1 921
（i） Online Business Fraud	*2 317*	*6 941*		1 040
（ii） Email Scam	*816*	*767*		93
（iii） E-banking Fraud	*3*	*0*		0
（iv） Social Media Deception	*1 678*	*1 988*		476
（v） Miscellaneous Fraud	*343*	*1 020*		312
Internet Blackmail	300	1 144	*+281*	142
（i） Naked Chat	*171*	*1 009*		119
（ii） Other Internet Blackmail	*129*	*135*		23
Misuse of Computer[2]	71	111	*+56*	14
Others	2 794	945	*-66*	81
Total (number of cases):	**8 322**	**12 916**	***+55***	**2 158**
Monetary Loss (in $ million):	**2,907**	**2,964**	***+2***	**511**

[2] Including account abuse, hacking activities and DDoS attacks