For discussion
on 19 April 2022

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. In the past two years, various industries have accelerated their digital transformation in order to adapt to the "new normal" amid the epidemic. While it brings new opportunities to the wider use of information technology (IT), it also poses greater challenges to information security. On the other hand, global cyber security threats against critical infrastructure, such as attacks at supply chain and Internet of Things (IoT), have also increased, posing security risks to individuals, enterprises and the society. Therefore, the Government and every sector of the community have to be more vigilant and continue to raise their awareness of cyber security and defensive capability, with a view to effectively addressing and mitigating the risks brought about by such cyber security threats.

Overall Situation of Information and Cyber Security

3. The Government has all along been actively responding to the information security challenges brought by the "new normal". The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) handled a total of 7 725 security incidents in 2021, representing a drop of approximately 7% from 2020. The main categories of information security incidents were phishing (3 737 cases) and botnets (3 479 cases) respectively. The breakdown of statistics on security incidents is at **Annex I**. As compared

with 2020, the number of phishing cases increased by 7%, where over 70% of the incidents involved online shopping or online banking. The number of botnet cases decreased by about 16% when compared with that in 2020. The main reason was believed to be the successful destruction of one of the world's largest botnets in 2020, thereby releasing those local devices infected with the virus from its control. In addition, the numbers of cases in relation to malicious software (including ransomware), hacker's intrusion or web defacement, and distributed denial-of-service (DDoS) attacks all recorded a downward trend.

4. The Hong Kong Police Force (HKPF) recorded a total of 16 159 technology crime cases in 2021, representing an increase of about 25% as compared with 12 916 cases in 2020. The average monetary loss per case continued to decrease from about $230,000 in 2020 to about $190,000, and the total amount of monetary loss remained at about $3 billion, similar to that in 2020. Among them, the monetary loss related to email fraud cases exceeded $1.5 billion, accounting for half of the technology crimes. Over 70% of the victims were small and medium enterprises (SMEs). The breakdown of technology crimes is at **Annex II**.

Information Security Measures in the Community

5. The Office of the Government Chief Information Officer (OGCIO), the Cyber Security and Technology Crime Bureau of HKPF, HKCERT, and the Hong Kong Internet Registration Corporation Limited (HKIRC) have all along been working closely to provide timely support in various aspects to public and private organisations as well as the general public in order to build a secure and reliable cyber environment for the community.

(I) Enhancing the capability of Hong Kong enterprises (in particular SMEs) in responding to various cyber attacks

Monitoring, preventing and responding to cyber threats and attacks

6. HKCERT continues to provide cyber security information to the Internet community in Hong Kong. In 2021, HKCERT issued more than 370 pieces of information and security recommendations, and provided a free 24-hour hotline for receiving security incident reports and offering advice on incident response and recovery. To support SMEs in responding to security incidents more effectively, HKCERT will publish an "Information Security

Incident Guidelines" specifically for SMEs later this year to introduce them, in a simple and comprehensible manner, on how to prevent and handle common cyber attacks.

7. HKCERT also joins hands with industry organisations of various sectors to organise activities to strengthen cyber security awareness and capability in defending against attacks, as well as to promote information security best practices. In 2021 alone, HKCERT organised 28 thematic seminars in collaboration with various trade associations, attracting over 2 600 practitioners from different sectors, including financial services, insurance, industry, education, retail, catering, IT, etc. In the coming year, HKCERT will continue to reach out to more SMEs through various industry and SME associations and provide timely services related to cyber security.

8. To assist SMEs in coping with potential information security risks with limited resources, HKIRC started to provide a free scanning service for SME's websites as early as 2019. The service includes checking whether the websites have security vulnerabilities, and providing scanning reports and recommendations. As of February 2022, HKIRC had inspected more than 3 700 websites of local SMEs. HKCERT also launched the "Check Your Cyber Security Readiness" online self-assessment tools in September 2021 to provide SMEs with a better understanding of their cyber security status and provide recommendations to assist them in uplifting their overall information security capability.

9. In order to lower the thresholds for employees of SMEs to acquire cyber security knowledge and to more appropriately apply the knowledge to their work, HKIRC will develop a variety of interesting and convenient training materials for SMEs' employees this year. To assist SMEs in raising cyber security awareness and providing cyber security training for their staff, the training content will be tailor-made according to the cyber risk topics and scenarios encountered by different sectors (e.g. manufacturing, retail, etc.) or job nature of employees (e.g. human resources, finance, etc.).

10. With the practice of work from home arrangement adopted by many enterprises, OGCIO and HKCERT issued relevant security advice and guidelines to the public through multiple channels, covering the secure use of video conferencing, security measures for remote work, etc., to assist users in maintaining a secure remote working environment. In light of the recent upsurge of the epidemic, HKCERT published an updated "Work from Home"

security in January 2022, reminding enterprises and work-from-home employees to beware of privacy and information security in the working environment, ensure the security of Wi-Fi networks and accounts, and take appropriate security measures for computer systems and mobile work devices to prevent cyber attacks.

11. Moreover, to assist SMEs in preventing email scams, HKPF launched an anti-email scam project named e-GUARD. HKPF also worked together with the University of Hong Kong to co-develop a Suspicious Email Detection System (V@nguard) to help SMEs identify suspicious emails automatically. The first phase of the system was released in January 2022 for free use by enterprises.

Financial Support

12. To tie in with the development of innovation and technology, the Government has been providing financial support to enhance the level of information security of enterprises. Through the Technology Voucher Programme (TVP), the Government subsidises local enterprises in using technological services and solutions. Local non-listed enterprises and organisations can apply for the funding to improve their productivity or upgrade and transform their business processes. Enterprises can also utilise the funding to enhance systems and implement cyber security measures, including defence against cyber attacks, disaster recovery solutions and managed security services (MSS) which has been gaining popularity recently. Since 2016, TVP has funded more than 450 projects related to the upgrading of information systems and cyber security. The relevant funding amount is about $67 million.

Cyber security information sharing

13. OGCIO continues to partner with HKIRC to support the operation of the cross-sector "Partnership Programme for Cyber Security Information Sharing" to promote the exchange of cyber security information among public and private organisations (in particular SMEs). As of February 2022, about 1 000 public and private organisations have joined the programme, covering a wide range of sectors including finance (covering around 130 banks) and insurance, public utilities, transport, medical care, telecommunications, innovation and technology (including information security), education, etc. We are also actively collaborating with the Insurance Authority to promote insurance industry's participation in the programme. Currently, there are more

than 50 insurance companies registered as members of the partnership programme. The platform also provides a public zone for members of the public to obtain security alerts and advice from experts.

14. The platform launched an Application Programming Interface (API) in July 2021 to enable member organisations to acquire cyber threat information in an automated manner. We will also continue to explore more channels (including free open sources and paid commercial sources) to obtain appropriate cyber security threat intelligence which could enable member organisations to defend against cyber attacks more rapidly.

(II) Public education

15. OGCIO provides information security advice to the public through various channels (including radio, social media, websites, etc.). In 2021, we broadcast multiple series of promotion clips through radio programmes, covering security awareness of IoT devices, secure use of mobile payment, protection against malware infection, password management, protection against phishing attacks, etc. In addition, OGCIO and Radio Television Hong Kong (RTHK) jointly produced two series of "InfoSec Tour". The topics were on email and SMS scams, and Internet etiquette respectively. They were broadcast on the online platform in February 2022 to raise public awareness of these topics.

16. OGCIO continues to organise school visits together with professional bodies. In the two school years of 2020/21 and 2021/22 (as at February 2022), about 30 physical or virtual school visits were conducted in total, conveying information security messages to over 5 200 teachers and students. In 2021, OGCIO delivered cyber security talks for elderly service centres either physically or virtually to enhance their security awareness. In the coming year, we will continue to disseminate information security messages to teachers, students and the elderly through suitable approaches taking into account the epidemic situation.

17. To raise the awareness of the community on information security and avoiding cyber pitfalls, HKPF comprehensively disseminated anti-scam messages by organising "Anti-Deception Month", launching "Anti-Deception Coordination Centre (ADCC) One-Stop Platform" website and organising the "CyberDefenders' Months". HKPF also launched a one-stop platform called

"CyberDefender" in August 2021 to raise public awareness of online fraud and unhealthy contents.

18. To enhance the public's knowledge of cyber security, OGCIO, HKPF and HKCERT organised a series of promotional activities, including webinars and competitions in 2021. With the increasing popularity of Quick Response Code (QR Code) in recent years, HKCERT also provided guidelines on the "Secure Use of QR Code" to remind the public of the associated security risks.

(III) Supporting national security education

19. OGCIO organised the annual "Build a Secure Cyberspace" information security promotional campaign in conjunction with HKPF and HKCERT in September 2021 to strengthen the understanding of organisations and the general public on cyber security and national security. They were reminded to behave prudently in the cyber world and jointly maintain cyber security in order to raise the law-abiding awareness of Hong Kong citizens and avoid falling into cyber pitfalls or even breaching the law inadvertently. This year, the Government will continue the work in this aspect.

(IV) International and Mainland cooperation

20. OGCIO and HKCERT have been actively cooperating with the Mainland and global computer emergency response centres. For instance, OGCIO and HKCERT continued to participate in the joint annual incident response drill organised by the Asia Pacific Computer Emergency Response Team in 2021 and test the capability in coordinating response to cross-border incidents together with 25 members from 19 different economies.

Manpower Development in Information Security

21. To attract talent to Hong Kong from around the world, the Government continues to implement the Technology Talent Admission Scheme (TechTAS) and streamline the admission procedure for technology talent (including that in cyber security) undertaking research and development work. This has expedited the admission of cyber security technology talent from different parts of the world.

22. HKPF, OGCIO and HKCERT jointly organised the Cyber Security Professionals Awards again in 2021 to recognise and motivate outstanding cyber security managers and practitioners, and provide a platform for experience sharing to professionalise their capabilities in preventing and detecting cyber security incidents and building an intact cyber ecosystem.

23. To enhance young people's knowledge and skills in cyber security and to raise their interest in this area of work, HKIRC organised the Cyber Youth Programme 2021 in May 2021. The programme attracted over 100 students from more than 56 secondary schools to attend a 4-day cyber security course and simulation training with contents covering cyber attacks and defence training, server vulnerabilities, system fundamentals, attack chains, etc.

24. Moreover, OGCIO sponsored the Hong Kong Productivity Council and HKCERT to jointly organise the "Hong Kong Cyber Security New Generation Capture the Flag Challenge (CTF) 2021" in November 2021 to enhance students' and young people's cyber security knowledge and their interest in participating in the information security industry. In addition to the categories for secondary schools and tertiary institutions, an open category was added and CTF experts from the Mainland, Macao and Korea were invited to participate and exchange ideas. The competition was well received with participation of over 940 students from local secondary schools and tertiary institutions and IT elites forming 315 teams.

Internal Measures to Tackle Cyber Security Threats in the Government

(I) *Information sharing and threat alerts*

25. For the Government internally, OGCIO continues to utilise big data technology to collect and analyse cyber threat information from different sources, conduct collation and evaluation, issue timely cyber threats alerts to bureaux and departments (B/Ds) to fix security vulnerabilities as soon as possible. In 2021, OGCIO issued over 170 security alerts in relation to computer system or software vulnerabilities, and required all B/Ds to take appropriate preventive measures in a timely manner in order to properly protect Government information systems and data assets.

(II) *Information security of work from home*

26. To tie in with the work from home arrangements for government staff, B/Ds may, in accordance with the "Government IT Security Policy and Guidelines", provide their staff with equipment such as notebook computers and mobile devices with security patches and anti-malware software installed and regularly updated. They can work from home by remotely accessing government networks and systems through secure communications channels (including encrypted Virtual Private Network (VPN) connections with two-factor authentication). OGCIO also reminded B/Ds in the early stage of the new wave of the epidemic outbreak in January 2022 of the precautions to be taken when arranging work from home to ensure the security of government systems and data.

27. In addition, OGCIO and B/Ds arrange regular trainings to promote staff awareness of cyber security, covering information related to remote access to government systems and networks. OGCIO also reminds departments and their staff from time to time of cyber security information including prevention of phishing attacks, security precautions in using video conferencing, etc. OGCIO also arranged a number of webinars and solution showcases to enhance the related knowledge of government staff.

(III) *Data security protection*

28. We are committed to safeguarding data security. Promulgated by the Security Bureau, the "Security Regulations" defines the security classification of government information and explicitly requires government departments to properly classify the information they hold, and take corresponding measures according to the classification to ensure that the information is fully protected in the course of storage and business operations. OGCIO also formulated a detailed "Government IT Security Policy and Guidelines" under the framework of the "Security Regulations" for compliance by all departments, and requires departments to strengthen their data protection measures to address different information security threats.

29. In the development of anti-epidemic related systems, such as the "StayHomeSafe" home quarantine system, the "LeaveHomeSafe" mobile application and the "Hong Kong Health Code" system, 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. The Government also consulted the Office of the Privacy Commissioner for Personal Data (PCPD) in a timely manner at different implementation stages of the projects, to ensure that the security of systems and data and the privacy of the general public are properly safeguarded.

(IV) *Staff training & technical support*

30. To strengthen the capability of B/Ds in defending and responding to cyber security incidents, OGCIO organises a large-scale inter-departmental cyber security drill every year. Moreover, to effectively combat phishing-related attacks, we launched a new round of "Phishing Drill Campaign" in January 2022. Apart from enhancing staff awareness of phishing through simulated phishing emails, we also launched the "Anti-Phishing Resource Centre" thematic website which includes educational videos, quizzes, etc. to introduce how to identify phishing emails and various common traps.

31. In 2021, OGCIO organised a number of seminars and solution showcases to enhance the information security knowledge of government officials. Last year, over 2 000 government officials took part in these events to learn about the latest cyber security trends and preventive measures. OGCIO also encourages staff to pursue internationally recognised information security certificates in order to consolidate their professional knowledge.

32. In addition, OGCIO would continue to assist B/Ds in conducting security and penetration testing for their online systems and websites through the network cum system testing platform. It could identify potential vulnerabilities and fix them as early as possible so as to uphold system security. In 2021, the testing platform conducted testing for more than 820 government websites. We are preparing to launch an updated platform to conduct more in-depth security testing for government online systems and mobile applications.

(V) *Compliance audits*

33. To ensure strict compliance with the security requirements of the Government, OGCIO regularly conducts independent information security compliance audits for B/Ds and offers advice to assist them in continuously improving their information security management systems to tackle emerging information security threats. The previous round of audits was completed in

December 2021 and the compliance audit reports were submitted to Heads of Departments for reference and follow-up. A new round of audits will commence in the second quarter of 2022.

Way Forward

34. To effectively enhance the community's overall defensive capability in cyber security, the Government will continue to actively collaborate with different stakeholders to enhance the awareness and defensive capability of the business sector, in particular SMEs, as well as the general public through various measures. Meanwhile, the Innovation and Technology Bureau (ITB) and OGCIO will continue to strengthen measures to enhance cyber security level within the Government. ITB and OGCIO would also support the Security Bureau in its preparatory work for enacting cyber security legislation to clearly define the cyber security responsibilities of critical information infrastructure operators and strengthen the protection of the operation and data of Hong Kong's network systems and critical infrastructure information systems, with a view to building Hong Kong into a safer and more secure smart city.

Advice Sought

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

Innovation and Technology Bureau
Office of the Government Chief Information Officer
April 2022

Annex I

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

Incident Category	2020		2021		
	Number of cases	**%**	**Number of cases**	**%**	**Compared with 2020 (%)**
Phishing (including phishing emails and websites)	3 483	*42*	3 737	*48*	*+7*
Botnet	4 154	*50*	3 479	*45*	*-16*
Malicious Software (including ransomware)	181	*2*	112	*1*	*-38*
Hacker Intrusion/Web Defacement	36	*<1*	19	*<1*	*-47*
Distributed Denial-of-Service (DDoS) Attacks	53	*<1*	10	*<1*	*-81*
Others[1]	439	*5*	368	*5*	*-16*
Total:	**8 346**	***100***	**7 725**	*100*	*-7*

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

Annex II

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

	2020	2021	
Case Nature	**Number of cases**	**Number of cases**	**Compared with 2020 (%)**
Internet Deception	10 716	13 859	*+29*
（i） Online Business Fraud	*6 941*	*6 491*	
（ii） Email Scam	*767*	*549*	
（iii） E-banking Fraud	*0*	*87*	
（iv） Social Media Deception	*1 988*	*3 638*	
（v） Miscellaneous Fraud	*1 020*	*3 094*	
Internet Blackmail	1 144	1 317	*+15*
（i） Naked Chat	*1 009*	*1 159*	
（ii） Other Internet Blackmail	*135*	*158*	
Misuse of Computer[2]	111	142	*+28*
Others	945	841	*-11*
Total (number of cases):	**12 916**	**16 159**	***+25***
Monetary Loss (in $ million):	**2,964**	**3,024**	***+2***

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