For discussion
on 13 January 2020

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 Government's work in information security in the past year.

Background

2. The wide adoption of information technology ("IT") can bring convenience to the public and improve quality of living. At the same time, the risks of the public, enterprises and the community being hacked have increased correspondingly. For Hong Kong to become a secure smart city, the Government, different sectors of the community and the general public must have knowledge of cyber risks so as to become more vigilant and take appropriate measures to protect their information systems and data assets, with a view to continuously improving the defence and response capability of the society as a whole.

Overall Situation of Information and Cyber Security

3. In recent years, the global cyber security landscape has been changing incessantly and hackers' modes of attack have become more diverse. The Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") handled a total of 8 827 security incidents in the first 11 months of 2019, which is equivalent to 88% of the total for 2018, showing a slight decline. The main categories of cyber security incidents in Hong Kong were botnets (4 570 cases), phishing (2 342 cases) and malware (1 205 cases). A breakdown of the security incidents is at **Annex I**. Both the numbers of botnets and phishing cases increased, by and large following the global cyber security trend. Most cyber attacks targeted system security vulnerabilities or insufficient user vigilance, with monetary gain as the main objective. Moreover, the increase in botnets also provided the basis for distributed denial-of-service ("DDoS") attacks. There

were 35 reported DDoS cases, showing a substantial increase as compared with 17 cases for the entire year of 2018. According to HKCERT, most of these cases were not attacks targeted at Hong Kong but originated from Hong Kong as reported by other regions. On the other hand, the number of malware incidents declined significantly in the past year.

4. The Hong Kong Police Force ("HKPF") recorded a total of 4 573 technology crime cases in the first three quarters of 2019, which is equivalent to 58% of the total of 2018, indicating a decline. However, the average monetary loss per case has increased from about $350,000 in 2018 to about $490,000. A breakdown of the concerned technology crimes is at **Annex II**.

Information Security Measures in the Community

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

5. The Government launched the Technology Voucher Programme ("TVP") in 2016 to encourage more local enterprises, including small and medium enterprises ("SMEs"), to make use of technology, including enhancement of cyber security measures to deal with cyber threats. Since February 2019, TVP has been regularised and further enhanced to increase its subsidy ceiling to $400,000 and the maximum number of approved projects for each enterprise from three to four. So far, TVP has approved over 150 applications involving upgrade of information systems and cyber security and the funding support amounted to about $18 million.

6. Unlike large enterprises, SMEs may not be able to allocate resources to defend against cyber attacks. Hence, the Government joined hands with the Hong Kong Internet Registration Corporation Limited ("HKIRC") to launch a free SME website scanning service to assist SMEs in identifying potential security vulnerabilities as early as possible. Apart from scanning malware in the system and providing information security improvement solutions for SMEs with ".hk" domain names, HKIRC also organises a number of seminars and workshops for them. Since its launch in June 2019, the service has received overwhelming response with about 300 local participating SMEs so far.

7. Moreover, given the importance of cyber security to individual sectors, HKCERT continues to join hands with relevant industry associations to organise thematic seminars to further promote cyber security awareness. In the past year, more than 20 seminars were held and attended by about 2 000 practitioners from

various sectors, including financial services, healthcare, retail and trade, property management, hotels and tourism, manufacturing, education, IT, etc.

(II) "Cyber Security Information Sharing and Collaborative Platform"

8. To promote the sharing of cyber risk information among industries and enterprises, the Office of the Government Chief Information Officer ("OGCIO") launched the "Pilot Partnership Programme for Cyber Security Information Sharing" in 2018 and took the lead to set up a cross-sector "Cyber Security Information Sharing and Collaborative Platform" (Cybersechub.hk). So far, about 150 public and private organisations have joined the programme, covering a wide range of sectors, including finance and insurance, public utilities, transport, healthcare, telecommunications, innovation and technology, information security, tertiary education institutions, etc. The platform enables the industries and enterprises to share information on cyber security threats, mitigation measures and best practices. It also provides an open section for the public to obtain security alerts and advice provided by experts. To encourage more public and private organisations to join the programme, OGCIO held the first anniversary celebration-cum-professional workshop for the programme in November 2019 to recognise the positive contributions by organisations and cyber security experts.

9. In view of the positive response from the participating members and industries, we have decided to regularise the programme and partner with HKIRC to promote the participation of more public and private organisations and sharing of cyber security information.

(III) Public education

10. In relation to the threat from phishing, OGCIO, HKPF and HKCERT conducted a series of promotional activities in 2019 under the theme "We Together! Secure Data!" to promote public awareness of information security, especially data protection. OGCIO has also disseminated different forms of cyber security information to the public through various channels, including websites, social media, printed media, etc.

11. To raise the youth's awareness in cyber security, HKPF organised the "Cyber's Got Talent Carnival" in March 2019 to educate the school community on the importance of cyber security for computers and mobile devices. OGCIO continues to organise school visits with professional bodies. In the 2018/19 school year, OGCIO conducted more than 40 visits and conveyed messages about information security to more than 10 000 teachers and students.

(IV) International cooperation

12. As Hong Kong is closely connected to the global network, we must respond quickly and effectively to cyber attacks from all over the world. OGCIO and HKCERT have been actively participating in global and regional security incident coordination centres, exchanging information on cyber security threats and responsive measures in order to disseminate timely warnings to all sectors of the community in Hong Kong. OGCIO also participated in the joint annual incident response drill conducted by the Asia Pacific Computer Emergency Response Team in July 2019 that aimed to enhance the incident response capabilities of various regions.

Manpower Resources in Information Security

13. With the continuous increase in cyber threats, the number of personnel responsible for information security and related duties in Hong Kong has also increased to around 4 200 people in 2019, representing an approximate 5% increase as compared to that of 2018. The Government will continue to encourage tertiary education institutions to introduce information security courses under different disciplines in order to sustain a stable supply of information security talent. In the area of professional training, we are also working with information security professional bodies to promote professional accreditation in order to nurture more IT practitioners with professional knowledge and skills in information security.

14. Furthermore, the Hong Kong Monetary Authority, the Hong Kong Institute of Bankers and the Hong Kong Applied Science and Technology Research Institute have jointly developed a localised certification scheme, namely, Certified Cyber Attack Simulation Professional ("CCASP"), and training programmes for cybersecurity professionals. The scheme is supported by the Council of Registered Ethical Security Testers ("CREST"), an international accreditation and certification body for information security located in the United Kingdom. It provides recognised professional training on cybersecurity. Between December 2016 and October 2019, a total of 55 persons passed its examination at various levels.

15. The Technology Talent Admission Scheme ("TechTAS") was launched in 2018 to provide a fast-track arrangement to admit overseas and the Mainland technology talent to undertake research and development work. As of end-December 2019, the Innovation and Technology Commission has allotted 26 quotas for cybersecurity-related job positions while the Immigration Department has approved eight visa / entry permit applications to cybersecurity

talent according to the relevant quotas. In addition, the Government announced in 2019 its decision to enhance TechTAS by expanding the scope of the scheme to research and development companies outside the Hong Kong Science & Technology Parks and Cyberport to allow more local technology companies to recruit technology talent from overseas and the Mainland to meet the demand of specific technology areas including cyber security. The implementation details of the enhancement measures will be announced shortly.

Internal Measures to Tackle Cyber Security Threats in the Government

(I) Information sharing and security alerts

16. In the past year, OGCIO strengthened the collection and analysis of cyber risk information from more sources and provided targeted and timely warnings to bureaux and departments ("B/Ds"). In 2019 (as of November), OGCIO issued some 90 security alerts in relation to computer systems or software vulnerabilities and requested B/Ds to take appropriate preventive measures promptly.

(II) Technical support

17. OGCIO established a new network and system-testing platform to assist B/Ds in conducting web page scanning and penetration testing. As of November 2019, the platform conducted testing for about 800 government websites. We will also organise training for support staff of B/Ds to enhance their knowledge and skills in managing emerging threats.

18. Given the worsening threat of phishing emails, the Government has implemented multiple layers of security measures and strengthened the security of government emails, hence facilitating the public to verify the authenticity of such emails so as to reduce the risk of government imposter scams. At the same time, OGCIO has utilised cloud computing technology to establish a modernised and centrally managed email system to ensure that better information security management practices are implemented by participating B/Ds, thereby further improving the reliability and security of email services within the Government.

(III) Staff training

19. The Government has put in place a set of incident response mechanism and measures, and conducts regular drills, including the annual large-scale inter-departmental cyber security drill exercise to enhance B/Ds' capability in responding to cyber security incidents. Additionally, OGCIO launched a ten-

month "Government-wide Phishing Drill Campaign" in May 2019. All government staff under the drill would receive simulated phishing emails and immediate feedback explaining the proper way to handle emails if the hyperlinks in these emails were clicked on. We also organised seminars, thematic websites, education videos and quizzes to introduce different ways to identify phishing emails and common pitfalls in order to deepen the understanding of phishing attacks among staff.

20. In 2019, OGCIO organised a number of seminars and solution showcases to enhance the knowledge of information security among civil servants. As of November 2019, more than 1 800 government staff took part in these events to understand the latest cyber security trends and preventive measures. OGCIO also encourages its staff to obtain internationally recognised information security certificates to strengthen their expertise in information security.

(IV) Compliance audits

21. To ensure that all B/Ds comply with the security requirements of the Government, OGCIO regularly conducts independent information security compliance audits and assist B/Ds in continuously improving their security management systems to tackle emerging security threats. OGCIO completed the previous round of audits for all government B/Ds in mid-2019. A new round of audits has been launched in November 2019 with a target of completing this regular audit exercise expeditiously within two years.

Way Forward

22. In view of the rapid development of technology such as artificial intelligence, big data and Internet of Things, OGCIO commenced a new round of review on the "Government IT Security Policy and Guidelines" in August 2019, covering the latest areas of information and cyber security as well as smart city development with reference to the latest international standards and industry best practices. We expect to complete the review within 2020 and publish the updated guidelines for general reference. The Government will continue to work with HKCERT, HKIRC and other stakeholders to further enhance the awareness and capability of various sectors of the community in cyber security and protection of personal privacy, so as to build a more secure cyberspace in Hong Kong.

Advice Sought

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

Innovation and Technology Bureau
Office of the Government Chief Information Officer
January 2020

Annex I

Breakdown of the Statistics on Security Incidents Handled by HKCERT

	2018		2019 (up to November)		
Incident category	**Number of cases**	**%**	**Number of cases**	**%**	**Compared with the entire year of 2018 (%)**
Hacker intrusion/web defacement	59	*<1%*	47	*<1%*	*80%*
Phishing (phishing emails and websites)	2 101	*21%*	2 342	*27%*	*111%*
Botnet	3 783	*37%*	4 570	*52%*	*121%*
Distributed Denial-of-Service (DDoS) attacks	17	*<1%*	35	*<1%*	*206%*
Malicious software (including ransomware)	3 181	*32%*	1 205	*14%*	*38%*
Others[1]	940	*9%*	628	*7%*	*67%*
Total:	**10 081**	***100%***	**8 827**	***100%***	***88%***

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

Annex II

Statistics on Technology-related Crimes Handled by HKPF and the Monetary Loss

	2018	2019 (Q1 – Q3)	
Case nature	**Number of cases**	**Number of cases**	**Compared with the entire year of 2018 (%)**
Online deception	6 354	3 861	61%
（i） Online business fraud	*2 717*	*1 686*	
（ii） Email scam	*894*	*604*	
（iii） E-banking fraud	*3*	*3*	
（iv） Social media deception	*2 064*	*1 332*	
（v） Miscellaneous fraud	*676*	*236*	
Online blackmail	504	255	51%
（i） Naked chat	*281*	*139*	
（ii） Other online blackmail	*223*	*116*	
Misuse of computer[2]	224	55	25%
Others	756	402	53%
Total (number of cases):	**7 838**	**4 573**	**58%**
Monetary loss (in $ million):	**2,771**	**2,248**	**81%**

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