For discussion
on 18 February 2019

Legislative Council
Panel on Information Technology and Broadcasting

Update on Information Security

Purpose

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

Background

2. While the popularity of information technology ("IT") has enhanced the quality of living and brought about various opportunities, it has also come with challenges. In order for Hong Kong to become a safe smart city, information security risks must not be overlooked. The Government, local enterprises and organisations, as well as the general public must stay vigilant at all times to protect their information systems and data assets. Nowadays, cyber attacks are on the rise and take different forms. Enterprises or organisations may not be able to cope with the evolving cyber threats on their own. Therefore, different sectors must foster close collaboration to share cyber security information and proactively learn about latest information security trends to take precautions and guard against cyber attacks. The Office of the Government Chief Information Officer ("OGCIO") has been tackling information security issues through a multi-pronged strategy, including the setting up of the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") to issue advices in relation to cyber security incidents and measures, protecting government information systems and critical information infrastructure, nurturing cyber security professionals and strengthening public education.

3. The Government established HKCERT in 2001, which is managed by the Hong Kong Productivity Council, to provide Hong Kong enterprises and Internet users with services related to computer security

incidents. These include collecting intelligence on information security threats and publishing latest information to enhance the public's security awareness, as well as providing advice on suggested measures to take in response to important security threats such as phishing attacks and ransomware. OGCIO also actively participates in global and regional computer emergency incident response organisations such as the "Forum of Incident Response and Security Teams" ("FIRST") and maintains close liaison with computer emergency response teams in other regions in order to get hold of cyber security information more quickly and comprehensively and take appropriate precautions.

Overall Situation of Information Security

4. According to an industry report[1], there was a rising trend of both phishing and data leakage incidents around the globe in the first six months of 2018. The information security situation in Hong Kong is in general in line with this trend, with an increase in the total number of security incidents in 2018. HKCERT received 10 081 security incident reports in 2018, representing an increase of about 55% as compared with 6 506 reports in 2017. Among these, the number of incidents in three main categories, i.e. botnet (3 783 cases), malware (3 181 cases[2]) and phishing (2 101 cases) have increased substantially.

5. On the other hand, the Hong Kong Police Force ("HKPF") recorded a total of 7 838 technology crime cases in 2018 with the total financial losses increased to around $2.77 billion, almost twice the amount of $1.39 billion in 2017. There was also a substantial increase in the average financial loss per case. The increase in technology crime cases was mainly due to the rise in the number of online frauds, Internet blackmailing and misuse of computers. There were also incidents involving leakage of customer data in large volumes owned by

[1] 2018 Midyear Security Roundup: Unseen Threats, Imminent Losses, Aug 2018, TrendMicro (https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/unseen-threats-imminent-losses)

[2] Including 114 ransomware reports and 2 426 Bot-WannaCry cases. The latter involved local computers being infected by the WannaCry ransomware which caused havoc on a global scale in May 2017, but the encryption programme was not activated and the infected computers did not incur any actual loss.

enterprises. A breakdown of the security incidents and technology crimes is at **Annex**.

Information Security Measures in the Community

Enhancing Capabilities of Local Enterprises to Tackle Various Cyber Attacks

6. According to a survey conducted by Hong Kong Productivity Council in 2018, the 350 surveyed local enterprises (including Small and Medium Enterprises ("SMEs")) from six industry sectors had adopted basic information security measures against cyber attacks in order to ensure smooth business operations and security of data assets. However, there still exists room for improvement in respect of security management and pro-activeness. To further strengthen security management of enterprises, OGCIO, HKPF and HKCERT have provided various support services to different sectors.

7. OGCIO and HKCERT have been monitoring closely trends of cyber attacks and related cyber threats, and reminding all organisations and the public timely to stay vigilant and take proper security measures for their computer equipment and data assets. In the past year, HKCERT issued 93 relevant security advices and guidelines, covering areas such as fixing product vulnerabilities, tackling ransomware attacks, preventing botnets, etc.

8. Having regard to the cyber attacks faced by specific sectors, HKCERT collaborates with relevant industry associations such as the Hong Kong Investment Funds Association, the Hong Kong Retail Management Association and the Travel Industry Council of Hong Kong, to publicise the importance of cyber security, promote information security best practices, and urge their member organisations to manage information security risks properly, as well as adopt various latest precautionary measures to appropriately handle and protect clients' personal data so as to boost public confidence in online services. Besides, HKPF regularly organises seminars on information security to strengthen the overall defence capabilities in handling cyber security

incidents across various sectors, such as banking and finance, transport and aviation, communications and public services.

9. To assist SMEs which have limited resources to cope with potential information security risks, HKCERT and OGCIO often collaborate with industry associations to organise relevant conferences, thematic seminars and workshops, covering topics like applications of cloud computing and artificial intelligence ("AI"). In 2018, OGCIO and HKCERT produced several series of promotional messages on information security issues that were commonly encountered by SMEs such as email frauds, malware, etc. for dissemination through various channels like social and electronic media.

10. The Innovation and Technology Commission expanded the scope of funding support and increased the level of subsidy for the Technology Voucher Scheme in February 2018. All local non-listed companies, including SMEs, can now apply for a subsidy to procure services and solutions to guard against cyber attacks and perform disaster recovery so as to further mitigate information security risks.

Pilot Partnership Programme for Cyber Security Information Sharing

11. OGCIO launched a two-year Pilot Partnership Programme for Cyber Security Information Sharing ("Pilot Partnership Programme") in September 2018 and took the lead to set up a cross-sector Cyber Security Information Sharing and Collaborative Platform (Cybersechub.hk). Through the platform, members of the Pilot Partnership Programme can exchange information on cyber security threats, mitigation solutions, best practices, etc., and disseminate relevant information to the public in a timely manner. To enhance the efficiency of information sharing, AI will also be incorporated into the platform to facilitate integration and analysis of cyber security information.

12. As at the end of 2018, more than 100 organisations have joined the Pilot Partnership Programme. We will continue to encourage more organisations from various sectors to join and collect their views to improve the programme. We will review the operation and

effectiveness of the Pilot Partnership Programme in the second half of this year for mapping out its way forward.

Public Awareness and Education

13. With the growing popularity of ICT devices and electronic payment services in recent years, related phishing attacks including fraudulent websites and phishing emails have also increased and take various forms. In view of the latest incidents and trends, OGCIO, HKPF and HKCERT organised a series of promotional activities in 2018 to raise public awareness against cyber frauds. These include cyber security seminars and promotional video contest which publicise messages of cyber security to enterprises, schools and the public, and enable them to master the relevant knowledge and skills.

14. To further assist the public in coping with phishing attacks, OGCIO set up a one-stop thematic web page "Beware of Phishing Attacks" under the "Cyber Security Information Portal". Its contents cover common types of attacks, related risks and impacts, detection and response strategies, recommended precautions, etc. OGCIO will continue to disseminate other information security messages to the public through the "Cyber Security Information Portal" and various promotional channels.

15. Following the first round of cyber security campaign in 2017 that aimed to tackle the potential security threats of botnets, HKPF launched the second round of the campaign in 2018 to raise public awareness in protection of mobile smart devices, and provide free-of-charge mobile anti-virus and scanning software to help protect their devices against cyber attacks including botnet and malicious software.

16. In the 2017/18 school year, OGCIO collaborated with professional bodies to organise school visits to enhance the knowledge of information security and promote the correct attitude towards the use of the Internet for over 9 100 teachers and students. In view of the positive response, we have continued to organise school visits in the 2018/19 school year. As of December 2018, we have conveyed information security messages to more than 5 900 teachers and students in the current school year.

Human Resources in Information Security

17. According to the 2018 Manpower Survey Report for Innovation and Technology Sector published by the Vocational Training Council, there were 95 780 professionals engaged in IT work, of whom some 4 000 were estimated to be performing information security and related duties. Given the latest information security situation, we consider it necessary to strengthen nurturing of talents in this field. The Government continues to collaborate with the industry to organise conferences, thematic seminars and workshops, including the annual "Information Security Summit", to encourage and support the industry in information security training. The Government also works with professional bodies to promote professional accreditation in information security among IT practitioners for enhancing their knowledge and skills in information security, and encourages them to join the information security profession with a view to nurturing more qualified professionals . In addition, the Government actively encourages tertiary education institutions to provide more information security courses in relevant disciplines to train up more talents with information security expertise and skills.

18. The Government launched the "Technology Talent Admission Scheme" in June 2018, which provides a fast-track arrangement for eligible technology companies and institutes to admit overseas and Mainland technology talents (including cyber security talents) to undertake research and development work. In addition, the Labour and Welfare Bureau announced in August 2018 the first Talent List of Hong Kong which put forward 11 professions, which can contribute to the development of Hong Kong as a high value-added and diversified economy, one of which is experienced cyber security specialist.

Internal Measures to Tackle Cyber Security Threats in Government

Compliance Audits and Policy Review

19. To protect Government information systems and data assets, OGCIO has, by making reference to international standards, formulated a comprehensive set of "Government IT Security Policy and Guidelines" ("Policy and Guidelines"). The Policy and Guidelines cover various areas, including information security management framework and security requirements for human resources, protection and encryption requirements for information systems and data assets, connection and access control, network and outsourcing service security, incident response and recovery, etc. To ensure bureaux and departments' (B/Ds') compliance with the requirements of the "Policy and Guidelines", OGCIO completed information security compliance audits of around 60 B/Ds in 2017 and 2018 and made recommendations for improvements. OGCIO will complete the compliance audits of the remaining B/Ds before mid-2019, and will launch a new round of compliance audits in the second half of this year.

20. To cope with the rapid technological development and emerging cyber threats, OGCIO will launch a new round of review of the "Policy and Guidelines" this year. The review will continue to make reference to the latest international standards and industry best practices, as well as to refine the security requirements in relevant areas by taking into account the latest landscape in information and cyber security.

Security Alerts

21. In view of the increasing cyber threats, OGCIO also implemented a cyber threat information sharing platform within the Government to strengthen the monitoring of cyber security threats and to share relevant information more effectively. In 2018, OGCIO issued about 100 security alerts related to computer systems or software vulnerabilities to remind B/Ds to take early and appropriate preventive measures.

Security Technology Measures

22. To protect Government information systems and websites against cyber attacks and intrusions, the Government has implemented multiple layers of security measures, including firewalls, anti-distributed denial-of-service solutions, intrusion detection and prevention systems, data encryption, anti-virus solutions, real-time monitoring tools, etc. OGCIO also reminds B/Ds from time to time to review the security controls of Government websites' operations, for instance, applying software updates to plug security vulnerabilities, checking system access logs, conducting regular security risk assessments and audits, etc. To meet the emerging information security challenges, OGCIO will continue to set up more network and system testing tools to assist B/Ds in reviewing their web page programme codes and conducting penetration tests in order to withstand attacks targeting at Government information systems and networks.

Incident Response and Security Drill

23. To raise B/Ds' awareness and response capability in tackling emerging cyber threats, OGCIO has since 2017 been co-organising with HKPF the annual inter-departmental cyber security drill, which strengthens the response capability of B/Ds through various simulated cyber attack scenarios. So far, all B/Ds have participated in the drill.

Civil Service Training

24. In 2018, OGCIO organised a number of seminars and solution showcases to provide proper training for over 1 800 departmental management personnel and information security staff. These training activities covered the latest cyber security trends such as security knowledge related to Internet of Things, smart city, phishing, etc. To strengthen the capability of police officers in responding to cyber attacks, the Cyber Security and Technology Crime Bureau under HKPF established the Cyber Range in December 2018. The Cyber Range is an advanced cyber security training and technical facility that provides trainees with hands-on experience through simulation of various cyber environments, attacks and scenarios.

25. With phishing becoming a major way of cyber attacks in recent years, OGCIO will arrange a series of activities, including seminars, thematic websites and anti-phishing drills this year to enhance the knowledge of Government personnel in defending against such attacks.

Looking Ahead

26. Cyber security threats have become one of the most significant security issues around the world, and Hong Kong must not lose sight. Apart from continuing to encourage more companies and organisations from different sectors to join the Pilot Partnership Programme, OGCIO and HKCERT will strengthen collaboration with HKPF and related organisations (such as the Office of the Privacy Commissioner for Personal Data and Hong Kong Internet Registration Corporation Limited) to further promote awareness and capabilities of the community in cyber security and protection of privacy, as well as render professional support to local enterprises in order to provide the community with a secure and reliable cyber environment.

Advice Sought

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

Innovation and Technology Bureau
Office of the Government Chief Information Officer
February 2019

Annex

Statistics on Security Incidents and Technology Crimes

Security Incidents Handled by HKCERT

Incident Category	**2017**		**2018**	
Hacker Intrusion/Web Defacement	26	*<1%*	59	*<1%*
Phishing	1 680	*26%*	2 101	*21%*
Botnet	2 084	*32%*	3 783	*37%*
Distributed Denial-of-Service (DDoS) Attacks	54	*1%*	17	*<1%*
Malicious Software (number of ransomware incidents)	2 041 (1 388)	*31%*	3 181 (2 540)	*32%*
Others	621	*10%*	940	*9%*
Total:	**6 506**	***100%***	**10 081**	***100%***

HKPF - Number of Technology related Crimes and Financial Loss

Case Nature	**2017**	**2018**
Internet Deception	4 231	6 354
(i) Online Business Fraud	*1 996*	*2 717*
(ii) Email Scam	*693*	*894*
(iii) E-banking Fraud	*0*	*3*
(iv) Social Media Deception	*1 063*	*2 064*
(v) Miscellaneous Fraud	*479*	*676*
Internet Blackmail	399	504
(i) Naked Chat	*305*	*281*
(ii) Other Internet Blackmail	*94*	*223*
Misuse of Computer	138	224
(i) Account Abuse	*92*	*174*
(ii) Hacking Activities	*37*	*47*
(iii) DDoS Attack	*9*	*3*
Others	799	756
Total (number of cases):	**5 567**	**7 838**
Loss (in HK$ million):	**1,393**	**2,771**