For discussion
on 12 February 2018

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 relevant measures implemented by the Government.

Background

2. As a major international and regional financial and business centre, Hong Kong is equipped with advanced information and communications technology facilities. With the rapid development of new technology applications such as online services, mobile payment, cloud services and smart home, the transmission of digital messages has become more frequent, which has also resulted in increasing associated information security risks.

3. The Government puts considerable emphasis on information security in Hong Kong and has been closely monitoring the trend of cyber attacks and security threats, making timely response and enhancing defensive measures. Through various channels, we have made known to all stakeholders (including the Government, enterprises and individuals) the trend of information security and the changing cyber environment, so that effective measures can be taken to protect their computer systems and information assets.

4. This paper reports the latest development and the work of the Government on information security over the past year in the following main areas:

(a) information and cyber security landscape;
(b) measures taken by the Government to tackle cyber security threats;
(c) information security measures in the community; and
(d) professional training and public awareness.

Information and Cyber Security Landscape

5. In 2017, computer security incidents took place on a global scale from time to time. According to a report published by a network security products company, the number of global ransomware attacks in the first six months of 2017 nearly doubled the figure during the same period of 2016. Subsequent to the widespread impact of WannaCry, other ransomwares (such as Petrwrap) also emerged, which suggests that the functions, complexity and techniques of ransomware are evolving constantly. In addition, the vulnerabilities found in the wireless network encryption protocol WPA2 and the Central Processing Unit design of computers may also induce hacker attacks and result in data theft. The frequent occurrence of computer security incidents of various kinds has not only increased the difficulties for stakeholders to address information and cyber threats, but has also raised public awareness of protecting sensitive information by various industries.

6. In general, there was an upward trend in the number of information security incidents in Hong Kong in 2017. A total of 6 506 incident reports were received by the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") throughout the year, representing an increase of about 7% when compared to 6 058 reports in 2016. Amongst the incident reports received in 2017, the number of malicious software attacks increased to 2 041, which is a marked increase of 79% when compared to 2016. Malicious software together with botnet (2 084 cases) and phishing (1 680 cases) have become the major categories of cyber security incidents in Hong Kong. Amongst the 2 041 malicious software attacks, 1 388 cases were related to ransomware[1].

[1] including 178 ransomware reports and 1 210 Bot-WannaCry cases. The latter involved local computers being infected by the WannaCry ransomware which caused havoc on a global scale last May, but the encryption program was not activated, and hence no actual loss was incurred.

7. On the other hand, the Hong Kong Police Force ("HKPF") recorded 5 567 technology crime cases in 2017 with a total financial loss of around $1.4 billion. Both figures have shown a decline when compared with 2016. A breakdown of computer security incidents and technology crimes is at **Annex**.

Measures Taken by the Government to Tackle Cyber Security Threats

Security Measures and Threat Alerts

8. Office of the Government Chief Information Officer ("OGCIO") closely monitors the daily operation of government systems, and scan, detect and defend them from any potential malicious attacks in order to ensure the normal operation of government computer systems. Internally, the Government has implemented multiple layers of security measures, including firewalls, intrusion detection and prevention systems, spam filtering systems, anti-virus solutions and real-time monitoring tools, to tackle external cyber attacks.

9. To further protect government websites, OGCIO has set up encrypted communication protocol for more than 120 government websites in 2017 to protect the public from data theft or data tampering by hackers when surfing government websites. On the other hand, to strengthen cyber security of government Internet services, OGCIO has also installed digital signatures for its hosted government Internet domain names in the second half of 2017 to protect the public from being re-directed to fake websites.

10. In 2017, OGCIO issued a total of 87 security alerts on computer systems and software vulnerabilities to government bureaux / departments ("B/Ds"), reminding them to take management and technical measures such as installing patches and updating system or software versions in a timely manner. OGCIO also assisted B/Ds in conducting scanning tests for over 500 government websites to block security vulnerabilities so as to protect government websites and data.

Guidelines Review and Audits

11. With reference to the latest international standards (ISO/IEC 27001/27002) and industry best practices, OGCIO completed a review of the "Government IT Security Policy and Guidelines" ("Guidelines") in end 2016 and promulgated the revised policy and guidelines to strengthen the requirements in different security areas, as well as updated and developed new guidelines. The revised policy and guidelines have been uploaded onto OGCIO's website for reference by the public and businesses.

12. With a view to assessing B/Ds' compliance with the Guidelines and providing them with recommendations for improvement, OGCIO launched a new round of security compliance audits in end 2016. During 2017, OGCIO completed compliance audits for 15 B/Ds. The whole exercise is expected to be completed by mid-2019.

Incident Response and Security Drills

13. The Government has put in place a set of incident response mechanism and measures, and conducts drills regularly. In case of security incidents, such as attacks targeting at individual B/Ds' websites, the departments concerned have to report forthwith and submit an incident investigation report to the Government Information Security Incident Response Office ("GIRO") of OGCIO, and report to HKPF immediately to facilitate their follow-up investigation.

14. To enhance the overall capability of the Government in handling cyber security incidents, OGCIO together with HKPF conducted cross-departmental cyber security drills in January 2017 and January 2018 respectively, in which around 60 government departments participated. Under a number of simulated scenarios, the participating departments experienced how to effectively respond to cyber security incidents, thus strengthening their capability in protecting information systems and handling such incidents. The drill will be conducted regularly every year.

International and Regional Cooperation

15. The Government Computer Emergency Response Team Hong Kong ("GovCERT") has all along been collaborating with computer emergency response teams of other places, including joining the "CERT Coordination Centre" ("CERT/CC"), the "Forum of Incident Response and Security Teams" ("FIRST"), and the "Asia Pacific Computer Emergency Response Team" ("APCERT"). To foster collaborative exchanges and sharing of information security intelligence, GovCERT actively participates in relevant activities organised by different organisations, including the CNCERT Annual Conference organised by the "National Computer Network Emergency Response Technical Team/Coordination Centre" ("CNCERT/CC"), annual conferences organised by CERT/CC and FIRST, and the joint annual incident response drill organised by APCERT.

Cyber Threat Information Sharing Platform

16. In response to the increasing cyber security threats, OGCIO launched a pilot project on cyber risk information sharing platform within the Government in April 2017, which utilised big data analytics technology to collect and analyse information on cyber security threats from different sources, and through collating and assessing the information, to provide B/Ds with more targeted alerts to cyber security threats.

Staff Training

17. The Government is committed to raising information security awareness and knowledge among staff. In 2017, OGCIO organised a number of seminars and solution showcases, providing appropriate training and learning opportunities for over 1 600 departmental management personnel and staff involved in information security. These activities covered such topics as industry best practices, ransomware and security of mobile applications. OGCIO will continue to organise these events to improve knowledge and skills of government officers about cyber security.

Information Security Measures in the Community

18. At the community level, OGCIO works closely with HKCERT and various stakeholders to render cyber security support to different sectors. The Cyber Security and Technology Crime Bureau ("CSTCB") under HKPF is dedicated to combating technology crime, enhancing the capability in handling major cyber security incidents or large-scale cyber attacks, and conducting timely cyber security threat audits and analysis so as to prevent and detect cyber attacks on critical infrastructure. CSTCB has been adopting a multi-agency approach in strengthening the reliability of critical infrastructure and enterprises' information system networks, as well as enhancing Hong Kong's capability of protecting relevant information system networks and defending against cyber attacks. HKCERT will also collaborate with organisations which provide Internet services to promote information security best practices in order to make Hong Kong a safe Internet hub.

Support for Specific Sectors on Cyber Security Awareness and Defence

19. In view of the recurrence of cyber security incidents involving travel agencies in recent months, HKCERT has been organising thematic seminars for the travel industry and other industries (such as retail and fund management) to enhance their cyber security awareness and capability to defend against such attacks. Meanwhile, the Travel Industry Council of Hong Kong will introduce various measures to further raise the cyber risk awareness of travel agencies, for example, organising cyber security seminars for their members, issuing notices to members, reaffirming the importance of cyber security etc. with a view to strengthening members' capabilities in cyber resilience and response to information security incidents. HKCERT will also continue to work with different industry associations to publicise and promote the importance of cyber security to the industries.

Enhancing Capabilities against Ransomware Attacks

20. In view of the rising trend of ransomware attacks in recent years, OGCIO has disseminated practical advice on guarding against ransomware attacks through the "Cyber Security Information Portal" (www.cybersecurity.hk). HKCERT has also published featured articles in newspapers, reminding the public of relevant security risks and defensive measures. A dedicated web page on ransomware has also been put up on the Portal to provide in-depth explanation of the hacking paths and impacts of different types of ransomware.

21. GovCERT and HKCERT jointly launched the "Fight Ransomware Campaign" in September 2017. The campaign included public seminars and the setting up of a "Ransomware Intelligence Portal" [2] on social media to share the latest intelligence and analysis, security alerts and training information, etc. As at December 2017, four public seminars have been conducted and nearly 30 articles have been released.

Support for SMEs

22. To strengthen the long-term competitiveness of SMEs, the Government has launched the $500 million Technology Voucher Programme ("TVP") on a pilot basis under the Innovation and Technology Fund in November 2016 to subsidise SMEs in using technology services and solutions to improve productivity or upgrade and transform their business processes. TVP also covers the adoption of cyber security solutions that provide SMEs with the means to defend against cyber attacks and disaster recovery solutions with a view to minimising the risks of incurring loss to their information systems. The three-year pilot programme provides a maximum subsidy of $200,000 for each eligible SME on a 2:1 matching basis.

[2] www.facebook.com/ransomware.hk

23. The adoption rate of cloud computing services among SMEs has been rising in recent years. In light of the potential security risks of cloud computing services, OGCIO has uploaded information on service providers under the Standing Offer Agreement for Quality Professional Services and cloud computing, as well as security and procurement guidelines on cloud computing services onto its cloud computing thematic website for reference by SMEs.

24. To promulgate information security knowledge in different areas and promote best practices to SMEs in a more effective manner, OGCIO produced several series of message announcement for broadcast on different electronic media in 2017 with topics covering ways to enhance website security, security tips on defending against ransomware and Distributed Denial-of-Service attacks, etc. with a view to encouraging SMEs' adoption of best practices to respond to cyber security challenges.

Professional Training and Public Awareness

Professional Training and Recognition

25. Since 2016, HKPF, GovCERT and HKCERT have co-organised the "Cyber Security Professionals Awards" ("CSPA") to recognise outstanding information technology ("IT") managers and practitioners for their contributions to the industry and encourage information security personnel to share their experience in order to enhance the industry's capability in cyber security protection. The 2nd CSPA presentation ceremony will be held in February 2018.

26. Regarding vocational training, the Hong Kong Productivity Council, HKCERT and GovCERT together with other organisations from time to time organise conferences, thematic seminars and workshops, including certificate courses on information security and the annual "Information Security Summit" to enhance IT practitioners' skills and knowledge of information security.

27. The Government also encourages tertiary institutions to provide more information security programmes in IT-related disciplines. We also continue to work with professional information security associations to promote professional accreditation among IT practitioners so as to train up more practitioners with professional knowledge and skills of information security, and encourage them to join the information security profession.

Raising Information Security Awareness among the Youth

28. With the popularity of mobile devices, cloud services and social media, the youth and students have more opportunities to access the Internet and IT equipment. Therefore, it is important to raise their awareness of cyber security. OGCIO has been collaborating with information security professional associations to organise school visits and "InfoSec" tours. In 2017, 32 school visits were conducted to reach out to nearly 10 000 students, parents and teachers. OGCIO will continue to organise school visits to instil in them the knowledge of information security and the proper attitude in using the Internet.

29. On the other hand, through actively organising various activities, the Government nurtures the interests of the youth in information security and discovers computer technology talents. To promote the message of "Cyber Security Starts from YOUth", HKPF and the University of Hong Kong continue to jointly organise the "Cyber Security Competition". The competition consisted of Tertiary Group, Secondary Group and Primary Group, attracting nearly 7 600 participants. The competition included online quiz, security vulnerability analysis in simulated computers and presentation on topics related to cyber security.

Public Awareness

30. With the development of smart city, Internet-connected devices are becoming more popular and diversified. OGCIO, HKPF and HKCERT organised two cyber security seminars with the theme of "Smart Home, Safe Living" in April and September 2017. The seminars aimed to help enterprises, schools and the public understand

the risks associated with Internet-connected devices, and remind them to stay vigilant to guard against security vulnerabilities as well as take appropriate security measures to ensure the safety of these devices and data. The seminar held in September 2017 covered topics such as defence against ransomware, the secure use of mobile payment and social media. Apart from organising seminars, OGCIO also disseminates messages about ransomware attacks, and provides relevant practical advice and risk mitigation solutions to the public through various channels, including social media, seminars, forums, information leaflets or pamphlets, television and radio broadcasts, and school visits.

31. To further assist the public in coping with cyber security threats, OGCIO has developed infographics on "Beware of Ransomware Infection", "Safe Online Shopping" and "Secure Your Home Network Devices", etc. with simple and practical security tips for reference by the public. OGCIO has also published learning programmes entitled "Protect Yourself against Ransomware" and "Safe Mobile Payment Services" through the "Cyber Security Information Portal". The Government will continue to release information security reference materials and messages to the public through the "InfoSec" website, the "Cyber Security Information Portal" and other promotional channels.

Looking Ahead

32. OGCIO will continue to facilitate the sharing of cyber risk information with the industry, enterprises and HKCERT, enhance exchange of cyber security threats to jointly defend against cyber attacks. OGCIO will implement a "Pilot Partnership Programme for Cyber Security Information Sharing" in the second quarter of 2018 for information security stakeholders, and launch its information sharing platform for cyber security in the second half of the year, with a view to promoting exchange of cyber security information among public and private organisations to strengthen Hong Kong's overall capability in defending against and recovering from cyber attacks.

33. The rapid development of emerging technologies such as IoT and electronic payment is spurring continuous innovation of our local services. However, it will also bring along different cyber security threats. Therefore, all stakeholders must remain vigilant. The Government will continue to enhance the knowledge of B/Ds, the industry and the public on the risks and threats of emerging technologies (including cloud computing, big data analytics, IoT, financial technology and artificial intelligence), as well as formulate and update related information security and technical requirements with reference to relevant policies in other regions, international standards and industry best practices.

Innovation and Technology Bureau
Office of the Government Chief Information Officer
February 2018

Annex

Statistics on Computer Security Incidents and Technology Crimes

Computer Security Incidents Handled by HKCERT

	2016		2017	
Hacker Intrusion/ Web Defacement	82	*1%*	26	*<1%*
Phishing	1 957	*32%*	1 680	*26%*
Botnet	2 028	*34%*	2 084	*32%*
Distributed Denial-of-Service	148	*2%*	54	*1%*
Malicious Software (the number of ransomware incidents)	1 139 (309)	*19%*	2 041 (1 388)	*31%*
Others	704	*12%*	621	*10%*
Total	**6 058**	***100%***	**6 506**	***100%***

Hong Kong Police Force - Technology Crimes and related Financial Loss

Case nature	**2016**	**2017**
Online game-related	363	311
Online business fraud	1 602	1 996
Unauthorised access to computers	1 107	822
Other Nature	2 867	2 438
(i) Miscellaneous Fraud	*1 563*	*1 542*
(ii) Child Pornography	*43*	*29*
(iii) DDoS Attacks	*6*	*9*
(iv) E-banking	*2*	*0*
(v) Naked Chat	*697*	*305*
(vi) Blackmail involving ransomware	*63*	*43*
(vii) Others	*493*	*510*
Total	**5 939**	**5 567**
Loss (in million $)	**2,300.8**	**1,393.0**