For discussion
on 12 December 2016

Legislative Council
Panel on Information Technology and Broadcasting
Update on Information Security

Purpose

This paper updates Members on the latest progress and development of the Government's information security programmes.

Background

2. Hong Kong is the world's freest economy and has an advanced information and communications technology infrastructure. With the vibrant development and wide adoption of smart phones, mobile devices and cloud services, Hong Kong is increasingly reliant on information and mobile technologies for economic development, entrepreneurship, business operation and daily life. With the rapid advancement of information technology ("IT") and increasing popularity of smart devices, the threats posed by information security and cyber attacks have brought impacts on businesses and other Internet users. For example, hackers may steal valuable information or disrupt the normal operation of computer systems. Therefore, all stakeholders (including the Government, businesses and individuals) should understand the risks in the cyber environment, acquire the relevant knowledge and take appropriate measures to protect their own information assets and computer systems.

3. This paper reports the latest developments of information security under the following main areas:

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

Information and Cyber Security Landscape

4. The Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") received a total of 5 146 incident reports during the period from January to October 2016. This represents an increase of nearly 4% as compared to 4 928 reports in the whole year of 2015. At the same time, according to the statistics from the Hong Kong Police Force ("HKPF"), a total of 4 537 technology crime reports were received in the first three quarters of 2016. Although the figure was slightly lower than that of the first three quarters of 2015 (5 333 cases), the estimated total financial loss has increased to around $1.9 billion, exceeding the total amount of last year ($1.8 billion). A breakdown of technology crimes and security incidents is set out at **Annex**. Although the number of incidents related to hacker intrusion/ web defacement, phishing, botnet and distributed denial-of-service attacks saw a downward trend, the number of local ransomware incidents has increased significantly. In the first ten months of 2016, there were 278 ransomware incidents reported, which was five times of the 51 incidents in last year, indicating that malware activities have been relatively active. All these reflect the changing variety of cyber threats and the need for corresponding changes in risk assessments and responsive actions.

5. With the advancement of technologies like big data, cloud computing, artificial intelligence, mobile devices and Internet of Things ("IoT"), cyber threats from around the world have become more diversified and sophisticated. Multiple reports from the information and cyber security industry[1] recently published revealed that malware is spreading rapidly across the globe in 2016 and has increased drastically in quantity, variety, performance and complexity. The global cyber threat landscape is much like that in Hong Kong, in which the number of ransomware incident reports has risen substantially over the past year. This makes the protection of computer data a focus in the area of information security. As a vibrant information society, Hong Kong is

---

[1] "2016 Midyear Security Roundup", Trend Micro Inc.
"Special Report: Ransomware and Business 2016", Symantec Corporation.
"H1 2016 Global and Regional Trends of the Most Wanted Malware", Check Point Software Technologies Ltd.

inevitably subject to these threats, and individuals, businesses and the Government are potential targets for attack.

6. In view of this, the Government, businesses and individuals must get well-prepared to cope with sudden cyber attacks and strengthen their security strategies so as to respond more effectively to such challenges. In addition to enhancing and regularly updating information security protection system, personal information security awareness and knowledge, as well as professional information security teams also play an important role in information security defense. As hackers can affect millions of users from anywhere in the world, it is necessary for us to strengthen international cooperation to share intelligence, coordinate investigations into suspicious activities and identify trends of emerging threats and cyber attacks. The Government attaches great importance to tackle the ever-changing cyber threats, and will continue to take various measures to enhance its cyber security. The related work is set out in the ensuing paragraphs.

Measures taken by the Government to tackle cyber security

7. The Government has been closely monitoring the trend of cyber attacks and related security threats. Within the Government, we have implemented multiple layers of security measures to withstand cyber security threats. By collecting cyber threat information issued by the cyber security industry and the Computer Emergency Response Teams ("CERTs") of other places, the Office of the Government Chief Information Officer ("OGCIO") timely disseminates security alerts and reminders to bureaux and departments ("B/Ds") and assists government IT staff and departmental emergency response teams in B/Ds to prepare for prompt response and strengthen their precautionary measures. OGCIO also organises seminars and training regularly for officers at various levels to strengthen their knowledge on cyber attacks and enhance their information security skills, thereby strengthening B/Ds' capabilities in guarding against such attacks.

Measures to Tackle Malware within the Government

8. Between January and October 2016, OGCIO issued 72 high-risk security alerts and 16 security reminders to B/Ds, including

two security guidelines related to ransomware. We have requested B/Ds to take effective and prompt responsive measures, and reminded all staff not to open suspicious emails and their attachments and links to prevent their computers from being infected. OGCIO has also reminded B/Ds to regularly use anti-malware software to scan their computer systems and perform data backup, and store the backup copy offline.

Risk Assessments and Audits

9. In view of the increasing number and complexity of cyber security threats, OGCIO will regularly review the relevant security requirements. With reference to the latest version of ISO 27001 international standards and other industry best practices, we have reviewed the "Government IT Security Policy and Guidelines", including increasing the confidentiality requirements for storage of sensitive information, strengthening departmental management capability for information security incident response, reviewing the capabilities of information security technology and detection of emerging cyber attacks, so as to address different types of information security threats and cyber attacks.

10. To assess B/Ds' compliance with the "Government IT Security Policy and Guidelines", OGCIO has since 2011 carried out independent information security compliance monitoring and audits for all B/Ds. During the course of assessment, we assist relevant B/Ds in continuously improving the security management systems and coping with emerging security threats. We will launch a new round of security compliance audits by the end of 2016. In addition, OGCIO also provides software and tools for B/Ds to conduct regular scanning on their websites in order to detect potential risks early and take appropriate preventive measures in a timely manner.

Incident Response and Security Drills

11. The Government has put in place a computer security incident response mechanism and associated measures, and conducts drills on a regular basis. From April to October 2016, OGCIO collaborated with HKPF in organising cyber security drills for

government departments to enhance the overall response capabilities of the Government in handling cyber security incidents.

Data Protection

12. To address the risks of data leakage, the Government has established stringent requirements and responsive measures on data protection, including the use of encryption with the highest industry standards when storing and transmitting sensitive data and documents to ensure the proper protection of government data assets. In addition, OGCIO has formulated practical guidelines and security requirements regarding the use of external storage devices to transport government documents and facilitated B/Ds to adopt appropriate technologies for encrypting government data.

13. To tackle the increasingly sophisticated and complex cyber security threats, OGCIO has requested B/Ds to strengthen data protection and develop systems to enhance their capacities in monitoring, detecting and blocking data leakage in the Government. B/Ds are also requested to monitor and analyse, and if necessary, block suspicious data flow in their networks.

International and Regional Cooperation

14. The Government Computer Emergency Response Team Hong Kong ("GovCERT.HK") maintains close liaison with other regional CERTs through joining the CERT Coordination Centre, the Forum of Incident Response and Security Teams, and the Asia Pacific Emergency Response Team ("APCERT") to facilitate timely sharing of information on security threats, vulnerabilities and security incidents. We also actively participate in technological exchange activities held by the organisations, including the APCERT Drill to be held in March 2017.

15. We also regularly participate in the meetings of the International Organization for Standardization on IT Security techniques (ISO/IEC JTC1/SC27) to follow the latest developments in technologies and standards related to information security.

Establishment of Big Data Analysis Platform

16. To address the increasing cyber security threats, OGCIO has planned to progressively strengthen the capabilities on monitoring cyber threats and sharing relevant information. Big data analytics technology will be used for establishing a cyber threat information sharing platform which can collect and analyse cyber threat information and data, detect potential incidents, provide more targeted cyber threat alerts to B/Ds, and promote sharing of cyber risk information among the industry, businesses and HKCERT so that all stakeholders (including the Government, businesses and individuals) can take early precautions and together reinforce Hong Kong's cyber security.

Staff Training

17. Raising information security awareness and knowledge among staff is instrumental to enhancing the overall information security level in the Government and protecting government information systems and data assets for reducing the risks of cyber attacks. In 2016, we have organised a total of 12 seminars, workshops and solution showcases for government IT staff and users to enhance their awareness of the latest security vulnerabilities and update their knowledge of information security technology. Among these events, four were related to ransomware threats with a view to strengthening the protection capabilities of staff in this regard.

Measures taken by the Community to Tackle Cyber Security Threats

18. OGCIO has been working closely with HKCERT and the industry to share information on security threats and vulnerabilities through various channels, including websites, newspapers, electronic media, mobile apps, public events and thematic talks. We have also provided security advice for protecting the information systems and data assets of the public.

Support for Small and Medium Enterprises ("SMEs")

19. In recent years, more and more SMEs expand their business

via e-commerce and e-payment platforms. However, if there are not enough security measures, their websites may be hacked or exploited as phishing websites and for hosting malware. In view of this, in early 2016, HKCERT launched the "SME Free Web Health Check Pilot Scheme" jointly with various local trade associations, including The Chinese Manufacturers' Association of Hong Kong, the Federation of Hong Kong Industries, the Hong Kong General Chamber of Commerce, the Hong Kong Small and Medium Enterprises Association and the SME One of the Hong Kong Productivity Council. Through this scheme, HKCERT promotes the "Check-Act-Verify" approach to SMEs, provides them with free website security checks and improvement suggestions, and conducts verification checks of their websites to confirm the effectiveness.

20. In mid-2016, HKCERT completed the first round of the checks and provided website security check reports and free consultation services to 30 participating SMEs. In August, seminars were held to share the findings and improvement suggestions. A second round of website checks to verify the effectiveness after improvements was also completed recently. Through this programme, SMEs can understand the security risks of their websites and enhance their website security. In 2017, OGCIO will continue to collaborate with HKCERT to organise related activities so as to raise the cyber security levels of SMEs.

21. To further enhance the information security awareness among SMEs and strengthen their defensive capabilities against cyber security threats, we have joined hands with the industry and different organisations to launch various publicity and education activities, including thematic seminars, radio programmes, distribution of information leaflets, etc., in order to remind businesses to strengthen cyber security measures and protect their information systems as well as data assets. We have also broadcast ten series of Announcements in the Public Interest on the radio covering various security tips to facilitate businesses and organisations to tackle cyber security challenges with industry best practices. In addition, OGCIO collaborated with HKPF and HKCERT in producing different thematic promotion leaflets to provide practical guidelines in helping SMEs formulate relevant security measures.

22. The adoption of cloud services among SMEs has been on the rise in recent years[2]. Having regard to the potential security risks of cloud services, OGCIO and the Support and Consultation Centre for SMEs of the Trade and Industry Department jointly organised the "SME's Cloud Security Forum" in September 2016. Through this seminar, SMEs and security experts shared and discussed the security considerations for cloud service acquisition and adoption.

Support for the Public to Tackle Malware

23. In the community, as the number of ransomware incidents in Hong Kong has increased drastically and posed serious threats to businesses and individual users, OGCIO, HKPF and HKCERT have organised seminars with the theme of "Protecting Data from Ransomware Attacks" for critical infrastructure operators, businesses and organisations, schools and the general public to enhance their understanding of the infection paths, impacts and processes of ransomware. Strategies and techniques in addressing ransomware attacks were also introduced.

24. Apart from organising seminars, we have also disseminated information on ransomware attacks to SMEs and the general public through the Cyber Security Information Portal (www.cybersecurity.hk), newspapers and electronic media. We have also provided related advice and risk mitigation measures, including a "Beware of Malware Infection" infographic to offer relevant security tips for reference. Besides, we have produced a learning module entitled "Protect Yourself against Ransomware" to introduce proper preventive and responsive measures with a view to reminding the public to take necessary precautions against ransomware attacks.

Public Awareness and Human Resources Development

Raising Information Security Awareness among the Youth

25. With the prevalence of mobile smart devices and wireless networks, coupled with the implementation of e-learning in schools,

[2] "2016 Cloud Readiness Index", Asia Cloud Computing Association.

youth and students now have more chances to access the Internet and computer equipment. Promoting information security to them has therefore become more important. This year, OGCIO continued to collaborate with information security professional organisations and conducted 30 school visits from January to October 2016, reaching out to nearly 10 000 students and teachers.

26. To increase the awareness among local primary, secondary and tertiary students on the safe use of the Internet and social media, and to scout computer and IT talents, HKPF and the University of Hong Kong jointly organised the first "Cyber Security Competition 2016" in Hong Kong during May to July 2016, to promote the message of "Cyber Security Starts from Youth". We will also continue to arrange school visits and other activities in order to educate local young people about the knowledge of information security and the proper attitude in using the Internet.

Promoting Development and Cooperation in the Information Security Industry

27. OGCIO proactively encourages the industry to participate in various kinds of cyber security events in order to understand the latest security threats and protective measures with a view to enhancing their professional competence. In April 2016, we held the "Hong Kong – Mainland Cyber Security Forum 2016" where cyber security experts of Hong Kong and the Mainland were invited to share their in-depth analysis on the cyber security challenges and associated technical solutions in the areas of financial technology, cloud computing, big data, etc., with over 200 industry practitioners.

28. To commend outstanding IT managers and practitioners for their contributions to the industry, OGCIO, HKPF and HKCERT co-organised the "Cyber Security Professionals Awards" in September 2016. This event aims at encouraging personnel who have contributed to the information security industry to share and exchange their insights in order to enhance the industry's capabilities of cyber security protection. This event was the first of its kind and had received over 160 nominations. The assessment work is in progress and the award presentation ceremony will be held in January 2017.

Public Awareness

29. OGCIO is committed to promoting information security awareness to various sectors in the community by collaborating with HKPF, HKCERT and other professional organisations to regularly hold various cyber security promotion events, including the annual event "Build a Secure Cyberspace 2016" to raise public awareness and capabilities of cyber security. This year, we have also organised three public seminars to allow the public to know more about the trend of cyber-attacks, remind them to stay vigilant against risks while making online transactions, and encourage them to strengthen the protection of personal and sensitive data.

30. Apart from organising public seminars, we held a Mascot Design Contest with the theme "Protect Data, Secure Transaction" during April to July to promote how to protect computer equipment and avoid falling into network trap, as well as the importance of data protection and online transaction security. The Contest received overwhelming response with over 2 000 entries. The award presentation ceremony was held in end November.

31. To allow the general users, SMEs and schools to receive the most updated security information, OGCIO has continually enriched the contents on the thematic Cyber Security Information Portal, e.g. featuring public events on information security, expert advice, information security stories contributed by professional organisations, etc., to provide practical tips and suggest useful tools for the public to protect their computer equipment and websites. Through the Portal, businesses and individuals could have a better understanding of potential security risks in the cyber world and the security measures to defend against Internet attacks.

32. OGCIO has been monitoring closely the latest status of cyber security threats. Following the launch of various mobile payment services, the development of mobile games and the recent cyber security incidents arising from IoT devices, we have included relevant topics and contents in various seminars and on the Cyber Security Information Portal to introduce the security risks involved in mobile games, mobile payment services and home network devices, and

to provide appropriate preventive measures and responsive solutions for risk mitigation.

Conclusion

33. Cyber attacks are no longer isolated issues and cyber threats are borderless and evolving. We need to forge closer ties and enhance information exchange with local and global organisations and professional bodies, continually monitor and understand the ever-changing cyber threats, explore feasible preventive and responsive measures, so that the Government and various parties can be well-prepared in tackling emerging cyber threats more effectively. We will continue to stay highly vigilant, keep a close watch on the prevailing security threats and adopt various measures with a view to protecting government information systems and data assets, enhancing security awareness in the community and collaborating with various stakeholders to jointly protect Hong Kong's cyber environment.

Innovation and Technology Bureau
Office of the Government Chief Information Officer
December 2016

Annex

Statistics on Security Incidents and Technology Crimes

Computer Security Incidents Handled by HKCERT

	2015		2016 (Up to October)	
Hacker Intrusion/ Web Defacement	151	*3%*	76	*1%*
Phishing	1 978	*40%*	1 635	*32%*
Botnet	1 943	*39%*	1 611	*31%*
Distributed Denial-of-Service	130	*3%*	94	*2%*
Malicious Software (the number of ransomware incidents)	277 (51)	*6%*	1 065 (278)	*21%*
Others	449	*9%*	665	*13%*
Total	**4 928**	***100%***	**5 146**	***100%***

Hong Kong Police Force - Technology Crimes and Financial Loss

Case nature		**2015**	**2016 (As at 30 Sept)**
Online game-related		416	304
Online business fraud		1 911	1 217
Unauthorised access to computers		1 223	847
Other Nature		3 312	2 169
(i)	*Miscellaneous Fraud*	*1 733*	*1 133*
(ii)	*Child Pornography*	*53*	*27*
(iii)	*DDoS Attacks*	*35*	*4*
(iv)	*E-banking*	*3*	*2*
(v)	*Naked Chat*	*1 098*	*588*
(vi)	*Others*	*390*	*415*
Total		**6 862**	**4 537**
Loss (in million $)		**1,828.9**	**1,865.2**