For Information
on 22 July 2014

Legislative Council Panel on Information Technology and Broadcasting

Information Security

Purpose

This paper updates Members on the latest progress of Government's information security programmes since July 2013.

Background

2. In the past year, we saw an increasing trend in the varieties and occurrence of information security threats and cyber attacks. The proliferated use of the Internet and mobile devices in conducting businesses and in daily life might be a major contributing factor. In 2013, the Hong Kong Police Force (HKPF) received 5 133 reports of technology crime, increased by over 70% from 3 015 reports in 2012, of which the number of "unauthorised access to computers" increased by 90%.

3. According to the "Hong Kong Security Watch Report" published by the Hong Kong Computer Emergency Response Team Coordination Center (HKCERT), there was an increasing trend of security events in the last four quarters. In the first quarter of 2014, the total number of security events exceeded 15 000, and in particular, the number of phishing and web defacement attacks increased significantly by 154%

to 2 039 and 97% to 3 490 respectively[1]. The cyber threats continue to grow in scale and sophistication.

Meeting the Challenges

4. The traditional roles and responsibilities of information security have been complicated by the various emerging cyber threats and it would not be enough for businesses and individuals to only protect their own information systems in isolation. They also need to master new skills to guard against cyber attacks and malicious activities over the Internet or mobile networks. The Government places heavy emphasis on information and cyber security.

5. Within Government, the Office of the Government Chief Information Officer (OGCIO) works proactively to –

- Protect government's information systems and data asset;
- Audit all bureaux and departments (B/Ds) on their security requirements compliance; and
- Review our computer emergency response mechanism and promote awareness and education on cyber security

6. In the wider community context, we actively –

- Collaborate with local and overseas stakeholders to strengthen the collection and sharing of security intelligence;
- Promote awareness and education in information and cyber security; and
- Promote public-private partnership to secure the cyberspace.

[1] https://www.hkcert.org/my_url/en/blog/14052101?nid=219283

Protecting government's information systems

7. The Government information systems are protected by appropriate and adequate security controls and measures in commensurate with their nature of services and risk levels. We have implemented security measures including intrusion detection and prevention systems, access control systems, firewalls, anti-virus solutions, to monitor, detect and block suspected traffic to our computer systems and networks. The Government Cloud Infrastructure and data centres are well protected by robust and secure solutions in full compliance with government security requirements and all data maintained are well protected by encryption technology. These installations are also accredited with international standards on International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 20000 - information technology service management and ISO/IEC 27001 - information security management system for quality assurance in operations management and security controls.

8. With a view to assuring that the implemented security measures are appropriate and adequate to meet the new challenges, regular security risk assessment of government websites are in place. In addition to the regular risk assessments performed by individual B/Ds, OGCIO is planning to launch a special exercise to health scan all public-facing government websites to reassure their security risk and defensive capabilities. We will also arrange advanced cyber security training for our information security practitioners in the Government and provide refresher training to system administrators with a view to enhancing overall cyber security capabilities and improve the knowledge and skills of our colleagues in addressing the challenges of emerging cyber threats.

Information security compliance audit

9. Security risk management is an important process that the Government deploys to proactively identify security risks and implement

appropriate security measures to mitigate the risks. In 2013-14, the Government invested $114.4 million for 122 security-related projects, which is a significant increase from $65.8 million for 85 projects in 2012-13. These projects include the conduct of security risk assessments and audits, implementation of technical solutions to enhance security controls, and upgrade of existing security infrastructures.

10. Since January 2011, OGCIO launched a dedicated programme to assess the compliance of B/Ds with the Government's security policy and requirements. As of June 2014, we have completed compliance audit on the critical systems of 42 B/Ds. The audit results showed that all these B/Ds complied with the government security policy and requirements, and they have learned through the process of the importance of continuous enhancement on their security management system to cope with emerging security threats. We will continue the compliance audit for all the remaining B/Ds in the coming two years.

Collection and sharing of security alerts and warnings

11. As an active participant in the cyber space, it is important for all stakeholders, including the Government, businesses and the public, to understand the associated risks and learn the skills to protect their information systems and sensitive data.

12. The Government's InfoSec portal (www.infosec.gov.hk) will continue to enrich its contents to assist the general public to effectively access information and resources on information security as well as measures and best practices for prevention of cyber crimes. We have also been distributing security alerts and warnings through emails and the GovHK Notifications mobile application.

13. Within Government, we monitor security threats and technology trends in order to introduce appropriate protection measures to safeguard government IT systems and information assets. In 2013-14, OGCIO

issued 63 high-threat security warnings and four security reminders to alert government users on prevailing or imminent security threats and advise them to take appropriate follow-up actions. We have also revised the Government's incident response mechanism to strengthen the incident response life cycle management to require all B/Ds to strictly follow the incident response requirement in prioritising resources to react to identified security events and implement appropriate remedial actions.

14. In the community, HKCERT is the centre for coordination of computer security incident response for local businesses and individuals. HKCERT coordinates with Computer Emergency Response Teams (CERTs) in other places of the world to disseminate security alerts and warnings as well as provide advice on preventive measures against security threats. In 2013-14, HKCERT published 443 security bulletins and 103 security blogs, increased from 439 and 78 respectively in 2012-13. The recent advisories on the Heartbleed flaw and eBay password issue have assisted local businesses and individuals to take remedial actions promptly. HKCERT has also published the "Hong Kong Security Watch Report" on a quarterly basis since the fourth quarter of 2013 to inform the public on the latest trends of identified security events and areas of concerns with appropriate advice on preventive measures.

Computer emergency response mechanism

15. With the objectives to enable smooth and efficient sharing of incidents identified in the region, we have revised the standing computer emergency response communication mechanism among OGCIO, HKPF, HKCERT, and local stakeholders to reinforce the roles and workflows among different parties in gathering cyber threats intelligence, sharing threat assessment, and incident response. The revised mechanism enhances the cooperation among various parties to facilitate timely and effective coordinated actions against cyber threats.

16. In facing the increasing trends of cyber threats and the potential public impact of targeted attack to government information systems and data assets, within Government, a task force comprising representatives from the OGCIO, the Security Bureau (SB) and HKPF has started to review the existing computer emergency response and incident handling management framework in the Government with a view to strengthening the cyber security capabilities. The Task Force will make reference to the best practices in other governments and recommend enhancement measures to strengthen the computer emergency response capabilities in the Government.

17. Cyber threats are borderless and it is therefore important to establish international collaboration for effective and efficient information sharing. OGCIO has been actively participating in international information security activities and cooperating with relevant institutions, including the Asia-Pacific Economic Cooperation and the Forum of Incident Response and Security Teams (FIRST) to establish working contacts with relevant experts at the international and regional levels to keep abreast of the latest news and trends on information security threats and defensive measures. We also collaborate with HKCERT to participate in the activities organised by the Asia Pacific Computer Emergency Response Team (APCERT). Relevant security information is disseminated to the community in a timely manner.

18. We have also joined HKCERT to study the functions and capabilities of the Computer Emergency Response Teams (CERTs) in other economies with a view to improving similar functions in Hong Kong, including the potential need for incorporating security profiling, sector-specific engagement, cyber threats detection, and proactive mode of operations in the existing mechanism to address emerging threats in the cyberspace.

Information security awareness and education

19. The human element is often regarded as the weakest link in information security. OGCIO endeavours to enhance citizens' knowledge to defend against cyber threats. In this regard, user awareness and knowledge on information security plays a crucial role. Our programmes cover both the Government and the community.

For Government Staff

20. OGCIO regularly arranges seminars and training courses for government staff to keep them up to date with the latest development in information security and develop their capabilities to better discharge their responsibilities.

21. To help B/Ds understand the latest security technologies and solutions, and raise their awareness on the need of protecting their systems and data, we have collaborated with the IT security industry to organise a series of IT Security Solution Showcases since November 2013. These showcases, combining presentations and booth demonstrations, presented to B/Ds dedicated security solutions and services to address specific security issues such as end point security, mobile security, encryption solutions, etc. We will continue to arrange thematic security solutions showcases in helping B/Ds to improve their security implementation continuously.

22. Training for IT support personnel is also crucial to B/Ds in carrying out their security tasks. In the past year, we have arranged over 60 in-depth security-related training courses attended by more than 400 IT security practitioners within government. As of June 2014, there are over 230 internationally recognised professional IT security certifications[2] acquired by personnel serving in various B/Ds.

[2] Professional security certifications include Certified Information Systems Security Professional (CISSP) offered by the International Information Systems Security Certification Consortium also known as (ISC)², Certified Information Systems Auditor (CISA) offered by the Information Systems Audit and Control Association (ISACA), etc.

23. In addition to the above, in 2013-14, we organised two security-specific seminars dedicated for officers responsible for information security in B/Ds. The objectives of these seminars are to ensure that these officers fully understand their roles and responsibilities, refresh their security knowledge of information and cyber security threats and mitigation measures, and reiterate the importance of protecting government's information systems and data assets in the cyberspace. We will continue to organise advanced security training and updates on government IT security policy regularly.

24. We will further develop the skills and capabilities of government IT professional staff on defending attacks against web applications. On-the-job training will be provided to build up cyber security capabilities of in-house security professionals involving in the penetration tests on web applications.

In the Community

25. Since 2005, OGCIO has been collaborating with HKPF and HKCERT to stage year-round activities in raising public awareness on information security. In 2013, the theme of the campaign was "Protecting from Targeted Attacks" and we have organised four public seminars to raise public awareness on the risk of targeted attacks. With the objective to reach the younger generation, we have organised a "Be a Smart Netizen" video contest to promote awareness of information security and adoption of best security practices in the community. The contest received encouraging responses. The winning entries not only demonstrate the creativity and passions of the participants, but also manifest the best practices in protecting computing devices against security threats.

26. In the coming year, OGCIO will continue to organise a thematic IT security education and promotional programme for the general public using various publicity channels. We are determined to ensure that IT

practitioners and IT users are better informed of the potential risks and what they can do to reduce them. We will also provide further guidance for the public on means to detect vulnerabilities on their computing devices and practical measures to protect themselves against cyber risks. From June to September 2014, we will organise a 4-panel comic contest with the theme "Information Security Starts from Me".

27. Awareness-raising activities in schools will continue at pace. In the coming year, in the light of the anticipated more extensive IT and WiFi adoption in schools under the IT in Education Strategy, we will further collaborate with professional organisations to develop training and workshops for technical support staff of schools so that they can better manage the computer systems, networks and data, and protect these facilities from cyber attacks.

Securing the cyberspace

Critical Information Infrastructures Protection

28. Critical infrastructures are increasingly dependent on IT in operations management and controls. Technical failures or cyber attacks would threaten the security and resilience of critical infrastructures. In this connection, HKPF established the Cyber Security Centre in 2012 to enhance protection of Hong Kong's critical infrastructures and strengthen Hong Kong's resilience capabilities against cyber attacks. HKPF plans to extend the roles and responsibilities of their existing Technology Crime Division to a new Cyber Security and Technology Crime Bureau in the latter part of 2014 with the objectives to strengthen HKPF's capabilities in protecting information systems of critical infrastructures as well as meet the various challenges of emerging technology crimes. The setting up of a new bureau in HKPF will be instrumental in raising the responsiveness and resilience against cyber attacks and incidents in Hong Kong.

29. We recognise the importance of public-private partnerships in

critical infrastructures protection. OGCIO established the Internet Infrastructure Liaison Group[3] in 2005 as a collaborative platform for the Government and critical information infrastructure stakeholders to share, contribute and collaborate in response to territory-wide incidents as well as to cooperate in maintaining the stability, security, availability and resilience of local Internet infrastructure for high-impact major events in the region.

30. Since 2009, OGCIO has collaborated with HKPF and HKCERT to co-organise annual cyber security drills with major Internet stakeholders. The focus of the drill exercise in 2013 was "Responding to Targeted Attacks". Participants included both fixed and mobile network providers, domain name registrars, and government B/Ds. The incident response procedures of participating parties were successfully tested. A drill would be conducted again later this year.

Adoption of International Security Standards and Best Practices

31. To guard against potential cyber attacks and cyber crimes, a comprehensive information security management mechanism is of particular importance to all organisations.

32. Within Government, our IT security policy and guidelines have been developed with reference to international security standards and industry best practices. B/Ds follow international information security management systems and comply with the requirements of the government security policy. In order to keep pace with the advancement of technology and address evolving security threats, we regularly review Government's information security requirements. We will start the next review exercise in mid-2015 to examine the latest security landscape and recommend necessary updates to these requirements.

[3] The Internet Infrastructure Liaison Group comprises members from Hong Kong Internet Exchange, Hong Kong Internet RegistrationCorporation Limited, Hong Kong Internet Service Providers Association, HKCERT, Office of the Communications Authority, HKPF and OGCIO.

33. At the community level, we encourage businesses to embrace international information security standards and best practices to protect their information systems and data assets. In April 2014, we hosted the ISO/IEC Joint Technical Committee 1/Sub-Committee 27 (SC 27) meeting in Hong Kong with a view to promoting wider adoption of international standards and best practices in the local IT industry. The ISO/IEC 27001 standards family, developed and managed by the SC 27, is a set of globally recognised information security management system standards. The meeting was attended by over 300 overseas and local security experts and professionals from more than 30 economies. Moreover, an industry event organised during the meeting period attracted some 400 participants including over 200 local attendees. The events have successfully raised security awareness and promoted wider adoption of international standards in information security in Hong Kong. We will continue the promotion activities to encourage the adoption of information security standards in strengthening our overall information security capabilities.

Collaboration with the Industry

34. In August 2013, OGCIO hosted a Roundtable to solicit expert views from leading local information security professionals, corporate users and academia on Hong Kong's capabilities and preparedness to guard against cyber threats. The meeting has discussed and explored ways to enhance Hong Kong's information security capabilities on information security governance, security threats detection and monitoring, incident response, talents development, and cross-sector collaboration.

35. During the International IT Fest 2014 held in April this year, three information security industry events were staged to provide platforms for overseas and local IT security professionals and IT practitioners to share and exchange their knowledge and experience. More than 350 participants attended these events.

36. Cloud services have grown in popularity worldwide. However, potential users, especially small and medium enterprises, may find it challenging to identify and procure the appropriate cloud services due to the lack of relevant knowledge and expertise. In April this year, we published on the InfoCloud portal (www.infocloud.gov.hk) a list of cloud service assessment tools and certification schemes, which can help cloud service providers to ascertain the security capabilities of their cloud service offers. Potential users, during service selection, can make reference to the information provided by cloud service providers through these tools and schemes. We are also collaborating with cloud experts of Guangdong Province on the development of a cloud security management scheme. Three local cloud service providers have been engaged to conduct a pilot testing on the scheme in 2014.

Conclusion

37. We stand ready to face the new challenges arising from the ever-evolving and challenging cyber threats. In addition to the established defense mechanism to protect our IT systems and information assets, we are taking proactive steps to build up the strength within the Government, across the business sector, and among the public. The Government will continue to safeguard Government's information systems and data, and working together with the industry and stakeholders for a safer cyberspace in Hong Kong.

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau
July 2014