For information
on 17 July 2015

Legislative Council Panel on Information Technology and Broadcasting

Information Security

Purpose

This paper updates Members on the progress and development of the Government's information security programmes since July 2014.

Background

2. The innovative use of information and communications technology (ICT), Internet services, and mobility solutions have greatly enhanced the quality of our daily lives. On the other hand, the proliferation of technologies and their wide adoption by businesses and the public also introduce complexity in the management of information security. With more businesses and sensitive information going online, it is essential for the public and private sectors, as well as individuals to join hands to guard against information security threats and cyber attacks.

3. In the past 12 months, the Government launched dedicated programmes to strengthen the security measures of its information systems and Internet infrastructures. We also collaborated with key stakeholders to raise public awareness and knowledge of information security through sharing best practices and guidelines in order to guard against malicious activities and cyber threats when going online. This paper summarises the developments under the following three areas:

(a) Information security trends and challenges;
(b) Key initiatives on safeguarding information security; and
(c) Information security awareness and education programmes.

Information Security Trends and Challenges

Increasing Cyber Security Threats

4. The increase in the number of cyber crimes and associated financial loss in 2014 indicated that cyber security threats are on the rise. According to the Hong Kong Police Force (HKPF), 6 778 technology crime cases were reported in 2014 representing a 30% increase over the 5 133 cases in 2013. The resulted total financial loss was estimated to increase from $0.9 billion in 2013 to $1.2 billion in 2014. This upward trend is also reflected in the figures of the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT). In 2014, the HKCERT received 3 443 security incident reports, more than double of the number (1 694) in 2013. Phishing incidents increased from 384 in 2013 by 55% to 594 in 2014.

5. In October 2014, there was a series of prolonged territory-wide cyber attacks on Hong Kong websites. The attacks involved web defacement, intrusion of networking and information systems, and distributed denial of service (DDoS) attacks targeting websites of the public and private sectors. Some one-click DDoS attack tools were available on the Internet for the manipulation of people without specialised knowledge. Normal operation of some websites was affected and resumed after the attacks subsided.

6. Apart from DDoS attacks, today's hackers can launch sophisticated cyber attacks including advanced targeted attacks, data

breaches and hacktivism. Globally, some high-profile incidents, such as hacking of a well-known movie and entertainment enterprise and an international bank have resulted in the loss of sensitive information. There was also an increasing number of local incident reports on "ransomware", which used crypto-software to encrypt the victim's computer files and asked for ransom in exchange for decryption keys. Such emerging threats, including targeted attacks through phishing electronic messages, impose great challenges to businesses and individuals alike.

Meeting the Challenges

7. The Government is committed to taking forward initiatives that can safeguard and strengthen the security of its information systems and data assets. In 2014-15, 114 security-related projects were initiated by bureaux and departments (B/Ds), incurring $139 million which was 22% higher than $114 million for the 122 security-related projects in 2013-14. These projects included conduct of security risk assessments and audits, implementation of technical security solutions, and upgrade of security infrastructures.

8. The Office of the Government Chief Information Officer (OGCIO) also works proactively with B/Ds to guard against malicious cyber activities and step up defensive efforts to protect the government information systems and data assets.

9. The Government's sensitive information including staff personal particulars and employment details must be classified. For classified information, the Government imposes stringent security requirements for B/Ds to follow. All classified information can only be processed on information systems complying with the Government's security regulations and must be encrypted during transmission. The

Government also keeps reviewing the security controls of classified information to cope with the advancement of technology and emerging cyber threats.

10. To raise public awareness, the OGCIO collaborates with the HKCERT and security service providers to gather information on security vulnerabilities and issue timely alerts on malicious cyber activities to the public and private sectors. In 2014, 46 early warnings and security alerts were disseminated through various channels including websites, mobile apps and social media.

11. We also coordinate with various stakeholders, including Internet service providers, the Hong Kong Internet Exchange, and the Hong Kong Internet Registration Corporation Limited, so as to strengthen protection against cyber attacks on critical information infrastructures. Besides, the HKCERT provides technical advice and assistance to the public when necessary.

Key Initiatives on Safeguarding Information Security

12. In view of the growing security threats and cyber attacks, we have implemented the following measures to enhance information and cyber security within the Government:

(a) Strengthening security controls and technical measures;
(b) Strengthening governance, risk management and the compliance framework;
(c) Conducting health checks on web services and drills on information security incidents;
(d) Enhancing computer emergency response mechanism; and
(e) Monitoring and responding to cyber threats and attacks.

Strengthening Security Controls and Technical Measures

13. The OGCIO gathered and analysed security intelligence from various reliable sources to provide B/Ds with timely alerts and advice on emerging threats. In 2014-15, we issued 76 high-threat security alerts and three security reminders to forewarn B/Ds on prevailing or imminent security threats, and advise them to take prompt precautionary and follow-up actions where necessary.

14. In addition, B/Ds have implemented multiple layers of security measures, including firewalls, intrusion detection and prevention systems, and real-time monitoring tools to guard against cyber attacks. When government networks and websites come under cyber attacks, technical staff, who monitor our systems round-the-clock, will take immediate actions to defend against intrusions into government computers and networks.

Strengthening Governance, Risk Management and the Compliance Framework

15. The OGCIO has formulated an information technology security policy and issued guidelines, which are based on international standards and industry best practices, on the use of IT within the Government. The policy was last reviewed in 2012. To address emerging security threats associated with the advancement of technology, we have started a new round of comprehensive review and will publish a revised set of IT security policy and guidelines by the end of 2016.

16. Since 2011, the OGCIO has launched an independent information security compliance monitoring and audit mechanism for assessing the compliance status of B/Ds. In 2014-15, we have completed audits for eight additional B/Ds and will complete the audit cycle for all B/Ds by August 2016.

Conducting Health Checks on Web Services and Drills on Information Security Incidents

17. From July 2014 to March 2015, the OGCIO conducted a centrally-coordinated vulnerability scanning for all government websites and a series of penetration tests for 100 mission-critical web applications. During this exercise, we set up central computer equipment and worked jointly with B/Ds to thoroughly examine and review the security measures of websites and web applications. Results revealed that B/Ds have put in place effective security measures to protect their websites and online services against cyber attacks.

18. The OGCIO collaborated with the HKPF and B/Ds to conduct cyber security drills for enhancing the overall incident response capabilities of the Government in tackling cyber security incidents. The drills kept the relevant security incident response teams, government staff and business partners conversant with the established security incident response and handling procedures. Reviews and sharing sessions were also conducted after the drills for subject officers of B/Ds to learn and share experience in best practices for making improvements. We will continue to arrange similar drills and related activities for B/Ds on mission-critical systems which are critical to the public and the Hong Kong economy.

Enhancing Computer Emergency Response Mechanism

19. As cyber attacks may threaten public online services, the OGCIO has enhanced the government-wide information security incident response mechanism and formed the Hong Kong Government Computer Emergency Response Team (GovCERT.HK) in April 2015 to proactively gather information on security threats and centrally coordinate incident responses. The GovCERT.HK will also work closely with the HKCERT

and other regional and global CERTs for coordinating threat information sharing and incident response.

20. In the community, the OGCIO established the Internet Infrastructure Liaison Group (IILG)[1] in 2005 to maintain close liaison with Internet infrastructure stakeholders and strive to sustain the healthy operation of the Internet infrastructure in Hong Kong in collaboration with industry players. In the past 12 months, we have activated the security alert mechanism four times to monitor and support events relating to cyber security incidents. We actively engage the stakeholders to promote closer collaboration in threat awareness and intelligence sharing.

21. The Cyber Security and Technology Crime Bureau (CSTCB) of the HKPF was established in January 2015 and is tasked to handle cyber security incidents and carry out technology crime investigations with law enforcement agencies both within and outside Hong Kong. In addition, the CSTCB will strive to raise the awareness of cyber security and technology crime prevention among critical infrastructure stakeholders, businesses, organisations and the general public.

Monitoring and Responding to Cyber Threats and Attacks

22. The OGCIO has been working closely with the HKCERT to monitor security threats and issue security alerts to the public. In 2014, the HKCERT issued 348 security bulletins and 126 security blogs to provide the public with timely information about prevailing security threats and vulnerabilities. The HKCERT also published the Hong Kong Security Watch Report on a quarterly basis to inform the public of the latest security status with advice on preventive measures. Through

[1] The IILG is chaired by Deputy Government Chief Information Officer (Consulting and Operations) with members including representatives from OGCIO, HKCERT, HKPF, Hong Kong Internet Exchange, Hong Kong Internet Registration Corporation Limited, Hong Kong Internet Service Providers Association and Office of the Communications Authority.

active collaboration with global security researchers and organisations, the HKCERT joined the global botnet takedown operations to fight cyber attacks and collected intelligence on compromised machines in Hong Kong. This exercise helps the public to discover and clean up "invisible botnets".

23. To strengthen the preparedness of key Internet players, we collaborated with the HKPF and the HKCERT to organise information security drills for Internet service providers, mobile operators and domain name registrars in October 2014. The theme of the drill exercise was "Strengthening Capability and Readiness against Cyber Attacks". Through various simulated incident scenarios, the drills tested the participants' capabilities of incident analysis, malware detection and malicious website tracking as well as their incident handling procedures.

Information Security Awareness and Education Programmes

24. People are often regarded as the weakest link in the IT security chain. User awareness of information security plays a vital role in coping with cyber threats. The OGCIO strives to promote information security awareness and education programmes for government staff and members of the public.

Enhancing Capability of Government Staff

25. To ensure that government staff remains vigilant in protecting their systems and safeguarding sensitive information, the OGCIO organised the following security awareness seminars and training in 2014-15:

(a) Nine security seminars and showcases were conducted for government IT staff and users to raise their security

awareness and introduce the latest IT security technologies and solutions. The topics included industry best practices, mobile and cyber security, data protection, end-point protection and anti-DDoS solutions;

(b) Two seminars were organised for departmental IT security officers to refresh their security knowledge and update them on the Government's latest approaches in dealing with cyber security threats and adopting mitigation measures; and

(c) Eight professional web application security training and sharing sessions for 800 government IT staff were arranged. The sessions specifically addressed common weaknesses of websites and web applications, and offered practical advice on the corresponding improvement measures to upkeep information security at a high level.

26. We will continue to arrange training and sharing activities to strengthen staff's capabilities in assuring information security within the Government.

Raising Public Awareness of Information Security

27. To raise public awareness and knowledge on the importance of information security, we have resorted to different publicity channels to reach out to different target audience and collaborated with the industry players in the process. The themes of last year's publicity programme were "Build a Secure Cyberspace" and "Information Security Starts from Me". Topics covered cyber security trends, cyber crimes and preventive measures, best practices of information security management, security tips on protection of personal information and mobile devices, etc. The target audience included businesses especially small and medium enterprises (SMEs); ICT practitioners; teachers, students and IT support staff of schools as well as the general public. Details are set out below:

(a) Six seminars were organised under the "Build a Secure Cyberspace" campaign with over 500 participants. The seminars aimed at promoting public awareness of information security and the adoption of security best practices;

(b) A security seminar with exhibition booths for SMEs was conducted to raise their awareness of cyber crimes and the need and measures to protect their information systems and data assets;

(c) Senior government officials also participated in 15 security seminars organised by the industry to share experience and information about trends of emerging threats and best practices of information security management with ICT practitioners;

(d) Ten school visits were arranged for over 2 000 students to raise their awareness of cyber security; and an information security week and training were arranged for some 600 teachers, school staff, technical support staff, and students to enhance their knowledge of protecting data, systems and networks;

(e) A four-panel comic drawing contest with the theme "Information Security Starts from Me" was conducted, aiming to encourage the public to proactively adopt security measures against cyber threats. The contest received overwhelming responses with over 1 800 entries covering different topics on information security. We published the winning entries of the contest on websites, newspapers and had them produced as booklets for distribution to the general public and schools;

(f) A thematic Cyber Security Information Portal (www.cybersecurity.hk) was launched in January 2015 with the objective to provide practical tips and advice, as well as useful tools for the general public to protect their computing devices and websites. With the information provided by the

portal, businesses and individuals can gain a better understanding of potential security risks in the cyber world and the security measures to guard against cyber attacks;

(g) A new series of Announcements in the Public Interest was broadcast in local TV and radio channels starting from February 2015 to promote proper online behaviour for protecting personal information and computing devices; and

(h) Social media, including YouTube and Twitter, were also used to share the best practices on cyber security and promote the upcoming security seminars and events.

28. In 2015, we will organise a graphic design contest with the theme "Cyber Security is Everywhere". We will continue to collaborate with professional organisations to enrich the content of the cyber security portal with more practical advice on cyber security, and make use of various publicity channels to promote and educate the public on the importance of cyber security.

Promoting Information Security Standards and Best Practices

29. Information security standards have been developed by international standards bodies devising practices and measures to cope with security threats. To enable effective security management, the Government adopts information security standards such as International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 and applies the corresponding techniques. We encourage the public and private sectors to adopt these standards to enhance information security awareness among staff, improve security operational efficiency, and strengthen the understanding of the need for continuous improvement.

30. To enhance the awareness of cloud computing services and security standards among various stakeholders, we continue to drive the

development and adoption of cloud computing through workshops, expert group meetings and the InfoCloud Portal (www.infocloud.gov.hk). In April 2015, with reference to the most recent ISO standards, we published "An Overview of ISO/IEC 27000 Family of Information Security Management System Standards" with a view to promoting wider adoption of international information security standards in Hong Kong.

Strengthening Local and International Collaboration

31. We recognise that collaboration on cyber security issues need to be firmly established between the Government and private sectors. To this end, we organised information sharing sessions so as to explore with the local industry on security issues facing businesses, collect information of specific incidents and threats detected by the industry, and share experience in adopting protection measures. In December 2014, we held two information security roundtable meetings with stakeholders of critical information infrastructures, telecommunications, and Internet service and data centre industries. The meetings have brought in useful insights and practical suggestions on measures to meet the security challenges and potential threats. We will continue to maintain close collaboration with the local industry.

32. To foster the Government's collaboration with international security experts for sharing experience in information security and strengthening knowledge of emerging cyber threats, vulnerabilities and appropriate mitigation technologies, the OGCIO keeps close contact with other governments and global organisations through our active participation in the Forum of Incident Response and Security Teams and the annual meeting of computer security incident response teams with national responsibility. The scope of sharing encompasses international standards development, global ICT security policies, and cyber crime initiatives and researches.

Conclusion

33. We will continue to stay vigilant and be aware of prevailing security threats, and implement various initiatives to safeguard Government's information systems and data assets, and promote public awareness in maintaining a secure local cyber environment.

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau
July 2015