For Information
on 8 July 2013

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 10 July 2012.

Background

2. The objectives of Government's information security programmes are to formulate and implement information security policies and guidelines for compliance and reference by bureaux and departments (B/Ds); ensure that all Government's information technology (IT)[1] infrastructure, systems and information are secure and resilient; and promote and enhance the awareness of information security and cyber risks among organisations and members of the public. Under these objectives, the Government continues to devote effort to strengthen its security protection capabilities, secure its computer systems and protect data privacy in the systems. We also work with all sectors in the community to help enhance their capabilities to protect their own computer systems and data. The updates provided in this paper cover three main areas –

(a) information security threats and risks;
(b) information security measures in the Government; and
(c) information security in the wider community.

[1] In this paper, information technology (IT) is used as an extended synonym for information and communications technology (ICT).

Information Security Threats and Risks

3. The proliferation of IT in modern society enables individuals, organisations, large enterprises and small companies to communicate and do business anytime, anywhere in a convenient and efficient fashion. However, the associated information security risks that could lead to data leakage or service outage are prominent. In 2012, the Hong Kong Computer Emergency Response Team Coordination Center (HKCERT) received 1 050 security incident reports and the majority of which was related to hacking and phishing. Compared to 2011, the number of incident reports increased by 30%. On crime statistics from the Hong Kong Police Force (HKPF), the number of technology crime cases in 2012 was 3 015, with the majority being unauthorised access to computer systems and online business fraud cases, up 37% from 2011. These figures indicated an upward trend of information security threats.

Information Security Measures in the Government

4. The Office of the Government Chief Information Officer (OGCIO) has formulated comprehensive security policies, guidelines and practices setting out the security requirements for protecting Government's computer systems and data. We require all Government bureaux and departments (B/Ds) to conduct regular departmental security risk assessment and implement governance mechanism on security compliance to help the B/Ds to identify security vulnerabilities and implement improvement measures. The OGCIO conducts sample check to verify the compliance level through visits and meetings with B/Ds. We also arrange information security seminars and training programmes to raise the security capabilities of staff. To protect against impending information security attacks and intrusion by hackers, B/Ds have adopted security best practices as highlighted below.

(a) Review of Government Information Security Requirements

5. In 2012, OGCIO, in collaboration with the Security Bureau, completed a review of the Government IT security related regulations, policies and guidelines. In the review exercise, security requirements related to the use of mobile devices, social networks and cloud computing were enhanced to reinforce the protection of Government information assets when using these new technologies. When enhancing our security requirements, we made reference to the security policies of other economies and prevailing international information security standards such as ISO 27001[2]. B/Ds were advised to review their departmental information security related policies and procedures to keep up with the updated security requirements. Security guidelines and best practices on mobile security, cloud security and privacy protection were enhanced and promulgated to B/Ds.

(b) Security Compliance and Risk Assessments

6. Since 2011, the OGCIO has visited 27 B/Ds and reviewed their respective security governance mechanism. Through the exercise, we work with B/Ds to verify security compliance and recommend actions to enhance security measures. In 2013-14, we will continue to visit another 15 B/Ds.

7. In 2012-13, there were 85 security-related projects initiated by B/Ds with objectives to enhance their security posture. The budget provision was $65.8 million, as compared to 71 projects costing $34.3 million in 2011-12. These projects included the conduct of security risk assessment and third-party audit as well as the implementation of technical solutions to enhance security and upgrade on existing security infrastructure.

[2] ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements is a Standard maintained by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

(c) Staff Education and Professional Development

8. It is important that all concerned staff understand the importance of information security measures and take responsibility to protect Government's systems and data. Our IT security policy requires that all staff shall be educated and trained periodically in order to develop their capabilities to discharge their responsibilities and perform their duties relating to IT security. The OGCIO makes use of various channels to promote information security awareness to staff. In 2012-13, we organised 10 security-related seminars and briefings[3] for over 1 400 participants. For IT practitioners, we arranged 54 in-depth security-related training courses for over 300 participants. For officers responsible for IT security in B/Ds, we will conduct a special training session for them in September this year to ensure that they fully understand their roles and responsibilities.

9. We reckon that security support personnel receiving formal training is beneficial to B/Ds for carrying out security initiatives. Currently there are about 200 internationally recognised professional security certifications[4] acquired by personnel serving in various B/Ds. To enable the sharing of knowledge and experience with international security experts, OGCIO staff also attends prominent international information security events, for example, the ISO/IEC JTC 1/SC 27[5] meeting and the the Forum of Incident Response and Security Teams (FIRST) conference in 2013.

10. With the wider adoption of Cloud computing, we issued in July 2012 a "Practice Guide on Cloud Security" to brief B/Ds on the security considerations and best practices for the adoption of Cloud services. We also issued in January 2013 a set of leaflets and posters reminding B/Ds

---

[3] Security-related seminars and briefings covered a variety of topics including "Protection of the Confidentiality, Integrity and Availability of Sensitive Data", "End Point Protection", "Mobile App Development with IT Security and Privacy in Mind" and "Cloud – A Security Perspective".

[4] 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.

[5] ISO/IEC JTC 1/SC 27 is the Joint Technical Committee 1 (JTC 1) Sub-Committee 27 (SC 27) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

the best practices of data protection when using mobile devices and removable media. The set of leaflets and posters has also been published on our information security portal (www.infosec.gov.hk) for public reference.

11. To keep B/Ds apprised of impending threats and enable them to be able to take prompt precautionary measures, we issue high-threat security alerts including possible cyber attacks and security reminders to demand B/Ds' immediate attention on need basis. In 2012-13, we issued 82 high-threat security alerts and three security reminders.

(d) Security Best Practices

12. To protect against impending information security attacks and intrusion by hackers, the Government continues to strengthen our security protection capabilities by adopting security best practices, including -

(i) installation of firewalls, anti-virus software and intrusion detection/prevention system at Internet gateways to protect critical systems against security threats;
(ii) timely update of system software and use of latest virus signatures to prevent infection of malware;
(iii) encryption of all confidential data during storage and transmission; and
(iv) conduct of regular security risk assessment and audit for critical IT systems.

The above practices have been effective in protecting our computer systems.

Information Security in the Wider Community

13. In relation to the community, the OGCIO carries out a number of activities in collaboration with industry players to promote the public's awareness of information security and adoption of best security practices.

(a) Information Security Awareness Promotion

14. Awareness on information security is of vital importance to empower users to withstand new and ever changing security threats. The OGCIO keeps abreast of global information security trend and development at all times and provides the public with abundant references and latest news on information security through the one-stop INFOSEC website. Furthermore, the OGCIO continued to organise a variety of activities throughout the past year to promote the awareness of information security and adoption of best security practices in the community. Since 2012, we have adopted the theme "Build a Secure Cyberspace" to promote public's awareness on strengthening the protection of their computing devices against cyber attacks through public seminars, radio programmes, website and a poster design contest. In 2013, four public seminars and a video contest will be organised with an aim to raise public attention on the importance to implement security measures to address cyber threats.

15. The OGCIO has always been supportive to information security programmes organised by the industry. In 2012-13, OGCIO attended eight public information security seminars organised by the local industry or professional associations and addressed the audience on information security.

(b) Adoption of Best Practices and International Standards

16. To promote public awareness on Cloud security to the public, large corporations and SMEs, we collaborated with the Expert Group on Cloud Computing Services and Standards[6] to develop two security checklists for reference by Cloud services consumers and providers. The two checklists, namely "Security checklists for cloud service consumers and solution providers" and "Security and privacy checklist

[6] The Expert Group on Cloud Computing Services and Standards was established by the OGCIO in April 2012 with members coming from the industry, academia and Government to help drive the cloud computing adoption and deployment in Hong Kong.

for cloud service providers in handling personal identifiable information in cloud platforms" were published through the dedicated thematic InfoCloud portal which was launched in January 2013. We will continue to collaborate with the industry to further promote the best practices.

17. The Government promotes and facilitates the development and adoption of international security standards and best practices in the industry. In April 2014, we will host the ISO/IEC JTC 1/SC 27 meeting in Hong Kong. The scope of SC 27 is the creation of standards for general methods and techniques in the area of information security. We expect that some 300 security experts and professionals from over 30 economies will meet and discuss the information security techniques and associated standards at the SC 27 meeting. The SC 27 managed standards, including the ISO 27001 and ISO 27002 standards, specify the requirement of an information security management system and provide best practice recommendations on information security management.

(c) Threat Response for the Community

18. HKCERT is the centre for coordination of computer security incident response for local enterprises and Internet users. Its missions are to facilitate information dissemination, provide advice on preventive measures against security threats and promote information security awareness. In 2012, HKCERT issued a total of 429 security alerts providing citizens timely information about current security threats and vulnerabilities. To enable users to stay tuned with important security messages using their mobile devices, HKCERT launched a mobile apps in May 2012 for citizens to receive the latest alerts and information. Since December 2012, security alerts from HKCERT have also been distributed via a new category "Information Security" under the "GovHK Notifications" mobile apps. As of early June 2013, the number of subscribers to this category was about 90 000.

19. With the growing trends of cyber attacks by Distributed Denial of Service (DDoS), HKCERT conducted a cyber security drill "Defending

Against Hacktivist Cyber Attack" in October 2012 to raise the preparedness of the participants[7] in handling such attacks. The incident response procedures of various parties had been successfully tested in the exercise. Another drill exercise is planned to be held later this year.

20. The OGCIO is collaborating closely with HKPF and HKCERT in exchanging intelligence on emerging security threats and taking collaborative measures to combat cyber attacks. The HKPF established the Cyber Security Centre (CSC) in December 2012 to enhance protection of Hong Kong's critical infrastructures and strengthen Hong Kong's resilience against cyber attacks. The CSC gathers cyber security related intelligence, and works closely with Government B/Ds, as well as local and overseas stakeholders. During the first five months of 2013, OGCIO coordinated with various parties on the handling of eight alleged attacks to Government services and assisted the concerned B/Ds to take proactive preventive measures to avoid service disruption.

Conclusion

21. 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, promote security awareness to the community in protecting the local cyber environment.

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau
July 2013

[7] Participants included network providers (fixed and mobile), Domain Name Registrars, Hong Kong Internet Registration Corporation; and Hong Kong Internet Service Providers Association together with Hong Kong Police Force, OGCIO and HKCERT