For Information
on 10 July 2012

Legislative Council Panel on Information Technology and Broadcasting

Information Security

Purpose

This is an update on the Government's information security programmes since 13 June 2011.

Background

2. The information security global trend continues to evolve as a result of emerging technologies and changing user behaviors. These also raise new issues for security. The Government continues to devote effort to strengthen its cyber security protection capabilities and help citizens protect their computer systems and data. The updates provided in this paper cover three main areas –

(a) information security global trend;
(b) information security initiatives in the Government; and
(c) information security in the wider community.

Information Security Global Trend

3. The widespread adoption of emerging technologies has an effect on information security. For example, people often focus on new features in mobile devices and convenience in connecting with friends using social networks, but they may not have put equal emphasis on security and privacy. This often provides opportunities for cyber criminals to exploit the vulnerabilities and conduct illicit activities. Another trend is that physical boundaries are disappearing as more business data are transmitted and stored outside the organisation with the deployment of mobile solutions and cloud services. In other words, securing the information systems of an organisation is no longer just

about firewalls and perimeter-based defences.

4. The number of network attacks detected by a security vendor in 2011 was twice as many as that in 2010[1]. The global phishing attacks[2] in 2011 recorded a 37% increase from 2010[3]. Infection by malicious apps on mobile platforms grew almost 40 folds from 400 in June 2011 to more than 15 000 in February 2012[4]. Hong Kong has been exposed to various cyber threats as in other parts of the world. According to the Hong Kong Police Force (HKPF), 2 206 cases of computer crime were reported in 2011, representing an increase of 34.3% as compared with the previous year[5].

Information Security Initiatives in the Government

5. The Office of the Government Chief Information Officer (OGCIO) puts heavy emphasis on information security within the Government. We continue to promote the awareness of information security amongst staff, identify technical tools and solutions to protect government's information systems and data, implement governance mechanism on security compliance, and review the existing security regulations, policies and guidelines. These are presented in the following paragraphs.

(a) Staff Awareness and Education

6. It is important that all staff understand the importance of information security measures and take responsibility to protect Government's information. The OGCIO makes use of various channels to promote information security awareness to staff. In 2011-12, we organised 10 security awareness seminars[6] attended by over 1 400 government staff, as compared with about 1 100 participants in 2010-11

---

[1] http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011

[2] Phishing attack is a cyber threat where someone with malicious intent makes use of fraud email or link directing users to fraudulent websites.

[3] http://www.rsa.com/phishing_reports.aspx

[4] http://www.devshed.com/c/a/Smartphone-Development/Juniper-Networks-Android-App-Malware-Increasing-11377/

[5] http://www.police.gov.hk/ppp_en/11_useful_info/doc/1213/SB-e032.pdf

[6] Security seminars covered a variety of topics including "Mobile Computing & Social Networking Security", "Web Application Security" and "Protection from Malware Attack".

for the same number of seminars. We also arranged 48 security-related training courses (including those convened in-house or through external providers) for attendance by about 400 government staff. 20 flash animations[7] have been produced and uploaded to the Government Intranet for staff's access to help them understand basic security knowledge and practices. Many bureaux and departments (B/Ds) drew references on these centrally developed training materials and bundled them into their own training tool kits for carrying out internal training and briefing.

7. The OGCIO closely monitors the information on cyber security made available by international and local organisations[8] to keep ourselves updated with the trends of attacks and solutions available in the market to guard against such attacks. In 2011-12, we issued six reminders covering various subjects including the protection of government websites and applications, and the protection of mobile devices; and disseminated 66 high threat alerts to B/Ds on security vulnerabilities. Similar to the 73 high threat alerts issued in 2010-11, they were mostly related to vulnerabilities found in operating systems, Internet browsers and media players. The alerts enabled B/Ds to take prompt actions to apply software fixes for effective protection of government information assets.

8. One of the effective communication channels with government staff is through the IT Security thematic website hosted on the Government Intranet, where there is a rich pool of resources on local and overseas news and alerts on security matters, security technologies and technical solutions, security policies, regulations and practice guides and other technical references. In a recent survey, 88% of B/Ds rated the website good or very good.

(b) Technical Tools and Solutions

9. The Government has adopted a systematic approach based on "Prevent, Detect, Respond and Recover" to protect our computer systems, network and information. B/Ds have implemented various technical

[7] Together with 20 flash animations produced in 2010-11, a total of 40 flash animations are available to help staff understand basic security knowledge and practices.

[8] These include local and overseas organisations responsible for incident response (e.g. US-CERT, HKCERT) and major anti-virus vendors.

security measures, such as firewalls, anti-virus software, intrusion detection/prevention systems and other security mechanisms to monitor, detect and block malicious codes and suspected traffic. Access control and encryption tools are used for protecting information from unauthorised access.

10. The OGCIO carries out market study and publishes technology updates and possible technical solutions on the Government Intranet for B/Ds' reference. There are currently more than 90 solutions under different categories, such as intrusion detection and prevention, secure network communication, security event management and virtualisation. With increasing popularity of mobile computing adoption, we have compiled reference information on solutions that place a greater emphasis on securing the data itself, such as data encryption, end point protection and data loss prevention solutions. We also promote adoption of public key infrastructure technology and use of digital certificates for secure communications and transactions.

(c) Security Compliance Governance

11. To oversee and enforce information security within the Government, an Information Security Management Committee (ISMC) with core members from the Security Bureau and the OGCIO was established in 2000 to provide security governance. An IT Security Working Group[9] was also set up as an executive arm of the ISMC in the promulgation and compliance monitoring of IT security policies and guidelines among B/Ds. In each B/D, a Departmental IT Security Officer is appointed who is responsible for the overall information security management and operation of the B/D concerned. In addition, an Information Security Incident Response Team is set up in every B/D to handle matters relating to security incident reporting and response, including stepping up the level of alert as and when necessary and conducting drills on a regular basis.

12. Since January 2011, the OGCIO has strengthened the compliance checking mechanism for better monitoring the security status of B/Ds. In 2011-12, the OGCIO completed compliance audit of 12

[9] IT Security Working Group comprises representatives from the Security Bureau, OGCIO, HKPF and Chief Secretary for Administration's Office.

B/Ds as planned. Through the exercise, we helped B/Ds to achieve compliance with the baseline IT security policy, identified risk items and improvement areas, and recommended actions to be followed up by the concerned B/Ds. In 2012-13, we plan to carry out compliance audit for another 14 B/Ds.

13. In the annual survey completed in June 2012, it was found that there were general improvements in the adoption of enhanced security measures and solutions to combat various security threats by B/Ds as compared with the previous year. For example, the use of end point security solutions that protect user computers and servers increased from 73% in 2011 to 82% in 2012; and the use of patch management solutions that facilitate deploying security software updates increased from 81% in 2011 to 88% in 2012.

14. We observed that B/Ds had placed much more priority in implementing security-related initiatives in 2011-12, including conducting security risk assessments and enhancing their security infrastructure. There were 71 security-related projects at an estimated expenditure of $34.3 million, as compared with 25 projects at $18.4 million in 2010-11.

(d) Review of Information Security Regulations, Policies and Guidelines

15. To ensure that the government IT security related regulations, policies and guidelines can keep in pace with the advancement of technology, the local and global security trends and the latest development of international/industry practices, OGCIO and the Security Bureau commenced a review exercise in November 2011. During the review, the government baseline IT security policy was benchmarked against those of other economies[10] and international standards[11]. From the benchmarking result, we identified a number of potential areas of changes which covered strengthening data protection, managing security under an outsourced environment as well as catering for emerging technologies such as mobile computing and use of cloud services. Based on these findings, new security requirements will be introduced on

[10] The economies included Australia, Canada, Japan, the United Kingdom and the United States.

[11] International standards included ISO27001 and ISO27002 (published by the International Organisation for Standardisation) and COBIT (Control Objectives for Information and related Technology published by the Information Systems Audit and Control Association).

the use of new technologies. We will promulgate the revised security regulations, policies and guidelines to B/Ds by the end of 2012.

Information Security in the Wider Community

16. Apart from initiatives within the Government, the OGCIO carries out a large number of activities in collaboration with other parties to promote the awareness of information security and adoption of best practices in the community, and enhance cyber security emergency response for security incidents. These are presented in the following paragraphs.

(a) Information Security Awareness Promotion

17. To raise public awareness on information security and strengthen the protection of personal computers and IT devices from cyber attacks, the OGCIO has organised an annual campaign covering contemporary topics in collaboration with the HKPF and the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) since 2005. The theme for the campaign in 2011 was mobile security and four public seminars were held attracting more than 500 participants. The campaign for 2012, en-titled "Build a Secure Cyber Space", focuses on security protection to combat cyber attacks. Four public seminars and a poster design contest will be organised.

18. To reach the wider community, the OGCIO produces, at a monthly interval, eight one-minute episodes on tips and best practices on information security topics requiring public attention[12]. These episodes are broadcast on the radio channel around three times daily.

(b) Promoting Adoption of Best Practices

19. The OGCIO publishes security best practices on our thematic website (www.infosec.gov.hk) and keep them up-to-date for public reference. The "Information Security Guide for Small Businesses" booklet with small and medium sized enterprises (SMEs) as our target

[12] Topics recently broadcast included "Tips for end-users when considering Cloud Service", "Safety tips on Online Social Networking", "Use Smartphone Securely" and "Use of Digital Certificates".

audience was distributed at public events and is also made available in the thematic website for public's reference and download.

20. For cloud computing, besides our own adoption in the Government, we also encourage its deployment in the private sector including SMEs. We have established an Expert Group on Cloud Computing Services and Standards in April 2012 with members coming from the industry, academia and Government to help drive the cloud computing adoption and deployment in Hong Kong. Given the importance of cloud security, we have formed a Working Group on Cloud Security and Privacy, amongst two others, under the main expert group. We will share the deliverables so produced with the local service providers and the private sector, SMEs in particular, so as to promote the wider adoption of cloud computing in a secure manner.

(c) Cyber Security Emergency Response

21. The Government recognises that a Computer Emergency Response Centre (CERC) is an essential component of a reliable and secure Internet infrastructure and has been providing financial support to Hong Kong Productivity Council for the provision of CERC services through HKCERT. Since 2001, HKCERT has been the centralised contact on computer and network security incident reporting and response. In case of security incidents, it helps local computer users to minimise services disruption, reduce loss and facilitate business operation recovery. In 2012, the OGCIO provided further funding support to HKCERT for expanding the Centre and strengthening its capability in closely monitoring abnormal activities on the Internet to uncover potential threats, issue alerts and kick-start preventive measures. To provide support on mobile security, HKCERT will also start in 2012-13 to include smartphone incident handling service to the public. Regarding overseas collaboration, HKCERT will maintain communication channels with other Computer Emergency Response Team (CERT) organisations and Forum of Incident Response and Security Team (FIRST)[13] to facilitate cooperation and coordination.

[13] FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programmes. It brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

22. With increasing phishing scams on popular web forums being discovered, HKCERT conducted a territory-wide drill in November 2011 to raise the preparedness of the administrators of local web forums in handling such threats. Three key players in the web forum community together with HKCERT, HKPF and OGCIO participated in the drill, which had successfully tested the incident response procedures of various parties.

Conclusion

23. We are facing new security challenges brought by the increasing use of mobile technology, cloud computing and social networking, as well as new threats in the cyber space. The Government will continue to carry out various information security initiatives for safeguarding Government's information systems and data, and protecting the local cyber environment. With the concerted effort of the ICT industry, information security practitioners, business organisations, the community and the Government, Hong Kong will stay in the forefront of a secure and reliable e-community.

Advice Sought

24. Members are invited to note the contents of this paper.

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau
July 2012