For Information
on 14 March 2016

Legislative Council
Panel on Information Technology and Broadcasting
Information Security

Purpose

This paper updates Members on the latest progress of the Government's information security programmes since July 2015.

Background

2. Hong Kong is a city with advanced telecommunications infrastructure and wide adoption of information and communications technology ("ICT"). The effective use of Internet services (including communication, mobile/smart devices and applications, e-banking, e-commerce, e-government and other forms of e-services) has greatly enhanced the people's quality of life and provided a strong foundation for economic development. On the other hand, the associated risks of information security and cyber threats have significant impacts on the smooth operation of businesses and Internet services. A reliable and secure cyber world is thus essential. It is important for all stakeholders, including the Government, businesses and individuals, to understand the risks, acquire the skills and take appropriate actions to protect their own information assets and ICT facilities.

Information Security Landscape

3. Information security and cyber threats are global issues and Hong Kong is no exception. An information security report[1] published in early 2016 has pointed out that coordinated attacks against governments and corporations worldwide continue to grow in complexity and strength. According to the IT Threat Evolution report[2] published by an international cyber security company in the third quarter of 2015,

[1] Akamai, Akamai Flash Report – Hacktivist, (February 2016)
[2] Kaspersky Lab, IT Threat Evolution in Q3 2015 Report

Hong Kong was ranked the 6th most targeted economy of online threat in the banking sector.

4. In 2015, the number of technology crimes reported to the Hong Kong Police Force ("HKPF") increased to 6 862 cases, as compared to 6 778 cases in 2014 and 5 133 cases in 2013. Although there was only a slight increase (about 1%) in the number of reported cases in 2015, the estimated total financial loss stood at $1.8 billion in 2015, which was an increase of 50% as compared to $1.2 billion in 2014. Besides disrupting critical business operations, recent incidents also revealed that more hackers are calling for ransom on critical business data being held hostage by crypto lockers.

5. The Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") handled 4 928 incident reports in 2015, representing an increase of 43% as compared to 3 443 incident reports in 2014. Among these, 1 978 incidents were related to phishing attack, representing a significant increase of 233% as compared to 594 cases in 2014. Phishing attacks are attempts to fake the victims for revealing their sensitive information such as bank account information, personal details and other private information.

6. This paper summarises the developments of the Government's information security programmes under the following main areas:

(a) information security in the Government;
(b) information security initiatives in the wider community; and
(c) public awareness and education.

Information Security in the Government

7. The Government is committed to protecting its information infrastructure and data assets. In 2015-16, 120 security-related projects were implemented by bureaux and departments ("B/Ds") and the estimated total expenditure was $106 million. These projects included conduct of security risk assessments and audits, implementation of technical security solutions and upgrading of security infrastructure.

IT Security Policy and Governance

8. The Government has put in place the "Government IT Security Policy and Guidelines" for compliance by B/Ds. In 2016, we will complete the review on prevailing security policies and guidelines with a view to strengthening the compliance requirements and security practices to cope with different types of emerging threats, such as malicious attacks, data leakage, network intrusions and phishing attacks.

9. The Office of the Government Chief Information Officer ("OGCIO") conducts "compliance audit" for B/Ds on a regular basis to ensure their compliance with the Government IT security regulations, policies and requirements. In 2015, we conducted compliance audits for 21 B/Ds to identify and address areas of improvement. In 2016, we will conduct compliance audits for around 20 more B/Ds.

Security Measures and Threat Alerts

10. In view of the high risks of distributed denial-of-service ("DDoS") and web defacement attacks, OGCIO has adopted proactive approaches in assisting B/Ds to implement appropriate protection measures and strengthen threat detection capabilities. All government websites are required to undergo more stringent security risk assessment and regular health checks, including vulnerability scanning and penetration testing. We also arrange training for the support personnel to update their knowledge on emerging threats and technical skills to mitigate risks.

11. Cyber threats can affect ICT facilities of various types. Therefore, it is essential to implement appropriate protection and detection measures to guard against potential information and cyber security threats. It is also critical to keep constant vigilance on imminent cyber attacks and issue timely alerts and advisories. In 2015, OGCIO issued 68 high-risk security alerts and eight security reminders to B/Ds, advising them to take management and technical measures to protect government websites and data.

12. To tackle increasing cyber security threats, OGCIO plans to further strengthen its capacity and capabilities on cyber threats surveillance and information sharing by forming a new team and re-allocating resources in mid-2016. We also plan to collaborate with the industry to establish a cyber threat information sharing platform in 2017 to proactively collect and analyse cyber threat information and data, and disseminate early warnings to B/Ds and the public.

Incident Response and Business Continuity

13. With the formation of the Government Computer Emergency Response Team Hong Kong ("GovCERT.HK") in April 2015, we continue to collaborate with HKPF in organising cyber security drills for B/Ds and stakeholders of Internet infrastructure. Through various simulated incident scenarios, we test the capabilities of incident analysis, standing incident response procedures and communication mechanism of the participants, and make continuous improvements. Since June 2015, we have conducted cyber security drills for eight B/Ds. We will continue to conduct drills in the coming year.

Capabilities Development

14. Within the Government, we have been encouraging staff to attend briefings, seminars, workshops, and professional training related to information security. In 2015, we have organised 12 training events for government users, administrators and IT professionals in order to raise their security awareness, and introduce to them the latest IT security technologies and solutions to enrich their knowledge in protecting the Government's information systems and sensitive information. In 2016, we will continue to organise information security related events for government staff.

Information Security Initiatives in the Wider Community

Protection of Internet Infrastructure

15. Since July 2015, we have activated the security alert mechanism of the Internet Infrastructure Liaison Group ("IILG")[3] three times to strengthen monitoring of cyber security of large-scale events and provide support events to protect the local Internet infrastructure against alleged cyber attacks. We will continue to actively engage the stakeholders to promote closer collaboration in threat awareness and intelligence sharing to maintain the stability, security, availability and resilience of the local Internet infrastructure.

Support for Small and Medium Enterprises ("SMEs")

16. With the development of the Internet and cloud technologies, many SMEs grasp the opportunities to expand their business on e-commerce platforms. OGCIO will provide funding support of about $10 million in 2016-17 for HKCERT to coordinate computer security incident response, monitor and disseminate security alerts, promote information security awareness to local enterprises and the public. We also work with HKCERT and relevant organisations to arrange seminars for SMEs to raise their awareness of cyber threats and share with them the best practices to manage information security risks.

17. HKCERT has launched the "SME Free Web Security Health Check Pilot Scheme" to promote awareness of information security and cyber threats to SMEs and help them build a more secure e-business environment. Through the project, HKCERT provides free website vulnerability scanning service for the participating SMEs and advises them on security improvements.

18. Moreover, we will work with HKCERT in the coming year to promote the "Check-Act-Verify" approach to SMEs, helping them

[3] OGCIO established the IILG in 2005 to maintain close liaison with Internet infrastructure stakeholders and strive to sustain the healthy operation of the Internet infrastructure. The IILG is chaired by the 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.

identify potential cyber threats, take improvement measures and verify the effectiveness of the measures with a view to enhancing the overall cyber security level of SMEs.

Collaboration with the Computer Emergency Response Teams ("CERT") Community

19. GovCERT.HK has been collaborating closely with HKCERT and CERTs of other places to share information on cyber security threats and coordinate incident response. It helps provide early warnings to the public.

20. In addition to sharing cyber security information, GovCERT.HK also participates in cooperative events with CERT community including sharing of knowledge and skills, training and workshops and cross-border incident response drills of a regional and global nature.

Public Awareness and Education

21. As cyber attacks continue to increase in number and sophistication, members of the public face cyber security risks when using different technologies, such as mobile devices, cloud services and social networking applications. We regularly arrange awareness training to share knowledge and latest best practices with the public, so that they can protect their computing devices and information assets by taking appropriate measures.

Publicity and Public Education

22. OGCIO will continue to collaborate with HKPF, HKCERT and other organisations to stage year-round activities in raising public awareness on information security. In 2015, the theme of the campaign was "Cyber Security is Everywhere". Three public seminars were organised with over 600 participants. The seminars aimed to remind the general public that they were surrounded by cyber threats and urge them to stay vigilant when using mobile devices or smartphones and take appropriate risk mitigation measures. As users are often the weakest

link in information security, we consider it necessary to promote the concept of "Security is Everyone's Business" to the public and private sectors through continuous education and awareness training. Moreover, we will continue to disseminate the latest security alerts and information to the public through our websites as well as other media and publicity channels.

Thematic Promotion

23. Another focus area of OGCIO's promotion programme in 2015 was on the security of mobile devices and applications. We broadcast seven radio tips on "Mobile Device Security" and "Mobile App Security" and cover the topics in our seminars. HKPF, the Hong Kong Monetary Authority and the Hong Kong Applied Science and Technology Research Institute will jointly organise a 3-day "Cyber Security Summit 2016" in May 2016 to share the strategies and technologies that support the protection of information systems of critical information infrastructure. The Summit will cover topics on the latest local and global trends of cyber attacks and organise workshops for various cyber security practitioners, particularly those from the financial sector.

Highlight Events

24. To maintain the vigilance of the public and students against cyber attacks, we organised a graphic design contest in 2015. The contest received overwhelming responses with over 1 500 entries. We will collaborate with HKPF and a local university to conduct a "Cyber Security Competition 2016" in mid-2016 for students of primary schools, secondary schools and higher education institutions. We also plan to arrange a week of promotional activities in September 2016, featuring school visits and mascot design contest, so as to raise awareness of information security among students, teenagers and the public.

School Education

25. It is crucial to promote proper attitude and practices to the young generation in using computing devices and managing personal

information. Since 2008, we have collaborated with Education Bureau and professional organisations in conducting school visits to raise the awareness of information security among students, teachers and parents, and provide them with advice on the protection of computing devices and personal information. From September 2015 to January 2016, we conducted around 30 school visits and reached out to over 12 000 students, teachers and parents. We will continue to arrange more school visits.

Professional Training and Certification

26. We encourage IT practitioners to attain recognised information security professional certifications, such as ISO/IEC 27001 Lead Auditor, Certified Information Systems Security Professional ("CISSP"), Certified Information Systems Auditor ("CISA") and Certified Information Security Manager ("CISM"). These certifications help enrich IT practitioners' security knowledge and enable them to perform their duties competently and enhance service quality. Besides sponsoring government staff to acquire these qualifications, OGCIO will collaborate with the industry to encourage their IT practitioners to acquire professional certifications.

Conclusion

27. The proliferation of hacking activities, coupled with the growing cyber threats associated with mobile devices, cloud computing, financial technology and targeted attacks on end-user devices, have posed ever-increasing challenges on cyber security. We will strive to work closely with various stakeholders to maintain a secure, stable and reliable e-government and e-business service environment.

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