立法會
Legislative Council

LC Paper No. CB(4)246/16-17(05)

Ref. : CB4/PL/ITB

Panel on Information Technology and Broadcasting

Meeting on 12 December 2016

Updated background brief on information security

Purpose

This paper gives a summary of views and concerns raised by Members during previous discussions on the Government's information security programmes.

Background

2. The objectives of the 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 the Government's information technology ("IT") infrastructure, systems and information are secure and resilient, and promote and enhance the awareness of information security and cyber risks among organizations and members of the public.

3. The Government has launched dedicated programmes to strengthen the security measures of its information systems and Internet infrastructures, and has collaborated with key stakeholders to raise public awareness and knowledge of information security through sharing best practices and guidelines. The developments of the Government's information security programmes were summarized under the following three 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

4. The Government is committed to protecting its information infrastructure and data assets. Security-related projects implemented by B/Ds included conduct of security risk assessments and audits, implementation of technical security solutions and upgrading of security infrastructure. For IT security policy and governance, the Government has put in place the "Government IT Security Policy and Guidelines" for compliance by B/Ds 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. 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.

5. In view of the high risks of distributed denial-of-service and web defacement attacks, OGCIO has adopted proactive approaches in assisting B/Ds to implement appropriate protection measures and strengthen threat detection capabilities, including vulnerability scanning and penetration testing. Training was also arranged for the support personnel to update their knowledge on emerging threats and technical skills to mitigate risks. OGCIO also keeps constant vigilance on imminent cyber attacks and issues timely alerts and advisories to B/Ds to take management and technical measures to protect government websites and data. OGCIO plans 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.

6. With the formation of the Government Computer Emergency Response Team Hong Kong ("GovCERT.HK") in April 2015, OGCIO continues to collaborate with the Hong Kong Police Force ("HKPF") in organizing cyber security drills for B/Ds and stakeholders of Internet infrastructure. Within the Government, staff have been encouraged to attend information security-related briefings, seminars, workshops and professional training. These training sessions aimed at raising their security awareness, and enriching their knowledge in the latest IT security technologies and solutions to protect the Government's information systems and sensitive information.

Information security initiatives in the wider community

7. For protection of Internet infrastructure, OGCIO has since July 2015 activated the security alert mechanism of the Internet Infrastructure Liaison

Group[1] ("IILG") 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. The Government has informed the Panel on Information Technology and Broadcasting ("the Panel") that it 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.

8. OGCIO had also provided funding support of about $10 million in 2016-2017 for Hong Kong Computer Emergency Response Team Coordination Centre [2] ("HKCERT") to coordinate computer security incident response, monitor and disseminate security alerts, promote information security awareness to local enterprises and the public. OGCIO works with HKCERT and relevant organizations to arrange seminars for small and medium enterprises ("SMEs") to raise their awareness of cyber threats, and share with them the best practices to manage information security risks. OGCIO also works with HKCERT to promote the "Check-Act-Verify" approach to SMEs, helping them 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.

9. 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 secured e-business environment. GovCERT.HK has been collaborating closely with HKCERT and CERTs of other places to share information on cyber security threats and coordinate incident response, and helps provide early warnings to the public. In addition to sharing cyber security information, GovCERT.HK also participates in cooperative events with the CERT community including sharing of knowledge and skills, training and workshops and cross-border incident response drills of a regional and global nature.

---

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

[2] Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT") is managed by the Hong Kong Productivity Council to coordinate computer security incident response for local enterprises and Internet Users.

Public awareness and education

10. As the public are exposed to cyber security risks when using different technologies such as mobile devices, cloud services and social networking applications, the Government regularly arranges awareness training to share knowledge and latest best practices with the public to protect their computing devices and information assets by taking appropriate measures. OGCIO has informed the Panel that it will continue to collaborate with HKPF, HKCERT and other organizations to stage year-round activities in raising public awareness on information security, including holding seminars to remind the general public that they were surrounded by cyber threats and urging them to take appropriate risk mitigation measures, and disseminating the latest security alerts and information to the public through the Government websites as well as other media and publicity channels.

11. On promotion and education, OGCIO broadcasts radio tips on "Mobile Device Security" and "Mobile App Security" and cover the topics in the seminars. HKPF, the Hong Kong Monetary Authority and the Hong Kong Applied Science and Technology Research Institute also jointly organized 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. Since 2008, OGCIO has collaborated with the Education Bureau and professional organizations 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.

12. On professional training and certification, apart from sponsoring government staff to acquire information security professional qualifications, OGCIO has informed the Panel that it will collaborate with the industry to encourage IT practitioners to acquire professional certifications.

Previous discussions

Panel on Information Technology and Broadcasting

13. At the Panel meeting held on 14 March 2016, the Administration briefed members on the progress and development of the Government's information security programmes since July 2015. Members' main concerns included information security landscape, implementing IT security policy and governance, protecting Internet infrastructure, collaborating with CERT community, raising public awareness and education as well as providing support for SMEs on information security.

Information security landscape

14. Some members expressed concern about the statistics on technology crimes and the financial loss caused by technology crimes. At the Panel's request, the Administration provided further information regarding the breakdown by nature of the financial loss caused by technology crimes in 2015, the detection rate of such crimes, and the breakdown by nature of incident, victims and financial loss of the incident reports handled by HKCERT in 2015. The Administration's written response was issued to the Panel vide LC Paper No. CB(4)958/15-16(01) on 9 May 2016 and is attached in **Appendix I**.

Implementing information technology security policy and governance

15. Noting that the Administration had reviewed the existing legislation and relevant administrative measures to deal with computer crime, some members expressed concerns whether the Innovation and Technology Bureau ("I&TB") would take over from the Security Bureau ("SB") to lead another review on information security issues. The Administration advised that it was regularly reviewing its information security policies, and would issue the "Government Information Technology Security Policy and Guidelines" in mid-2016 for B/Ds in handling Government information. The Administration also informed Panel members that I&TB would continue to work with SB on the formulation of information security policy.

Protecting Internet infrastructure

16. Some members expressed concerns about the safety and reliability of the Government's Internet of Things devices. The Administration advised that B/Ds would conduct regular reviews to ensure that their IT systems complied with the Government security requirements. Members were also informed that the Administration had engaged internationally accredited security experts in 2014-2015 to perform vulnerability scanning and penetration tests on the Government's Internet application systems. The results confirmed the capability of the Government's Internet application systems to withstand cyber attacks.

17. Some members raised concerns whether the Administration would conduct compliance audit for B/Ds more frequently than every four years to ensure that they had conducted their internal system audits in accordance with the Government's IT security regulations and requirements. The Administration advised that compliance audit exercises were resource-intensive and it was considered appropriate to conduct them on a four-year cycle basis. The Administration supplemented that more frequent compliance audit might be considered in respect of individual B/Ds where circumstances warranted.

Collaborating with Computer Emergency Response Teams community

18. Some members enquired about the cooperation between the Administration with IT security authorities of other jurisdictions in dealing with cyber attacks on government IT infrastructures. The Administration advised that GovCERT.HK had been collaborating closely with similar set-ups in the Asia Pacific region, Macau and the Mainland to share information on cyber security threats and coordinate incident response. In addition to sharing cyber security information, GovCERT.HK also participated in cooperative events with other computer emergency response teams for knowledge and skills sharing, training and cross-border incident response drills of a regional and global nature.

Raising public awareness and education and providing support for small and medium enterprises on information security

19. Some members expressed concerns about the need to raise the awareness of the younger generation about the risk of breaching the law inadvertently when using Internet social media. Members also queried the Administration's efforts in supporting SMEs in ensuring information security in day-to-day operations. The Administration advised that school visits had been conducted with the objectives of raising the awareness of students, teachers and parents on information security, and advising them on the importance of protecting computing devices and personal information. The Administration would organize and arrange seminars for SMEs to raise their awareness of cyber threats and share with them the best practices to manage information security risks.

Finance Committee

20. At the special meeting of the Finance Committee on 7 April 2016, Hon Charles Peter MOK enquired about, inter alia, the number of cyber attacks targeting government networks and websites in 2015-2016, the expenditure of Government B/Ds for security risk assessments and audits in 2015-2016, and whether information security risk assessments and checks had been performed for websites, applications and mobile applications developed by B/Ds in 2015-2016. Hon SIN Chung-kai also enquired about the expenditure and details on conducting security checking for government websites and web applications. The Administration's replies are in **Appendix II**.

Latest position

21. The Administration will brief the Panel on 12 December 2016 on the progress and development of the Government's information security programmes.

Relevant papers

22. A list of the relevant papers with their hyperlinks is at:

http://www.legco.gov.hk/yr15-16/english/panels/itb/papers/itb20160314cb4-689-3-e.pdf
http://www.legco.gov.hk/yr15-16/english/panels/itb/papers/itb20160314cb4-689-4-e.pdf
http://www.legco.gov.hk/yr15-16/english/panels/itb/minutes/itb20160314.pdf
http://www.legco.gov.hk/yr15-16/english/panels/itb/papers/itb20160314cb4-958-1-e.pdf
http://www.legco.gov.hk/yr15-16/english/fc/fc/w_q/itb-e.pdf

Council Business Division 4
Legislative Council Secretariat
7 December 2016

Appendix I

Information Requested by
the Panel on Information Technology and Broadcasting
on 14 March 2016

(a) Breakdown of the financial loss caused by technology crimes in 2015 is listed below:

Technology Crime Related Cases in 2015	Number of Cases	Financial Loss ($ Million)
Online Game	416	2.4
Online Business Fraud	1 911	40.4
Unauthorised Access to Computer System	1 223	1 462.4
Social Media Deception	1 422	60.0
Distributed Denial-of-Service	35	0.1
Others	1 855	263.6
Total	**6 862**	**1 828.9**

Of the 6 862 technology crime cases, 904 cases were detected and the detection rate was 13.2%.

(b) Breakdown of security incidents handled by the HKCERT in 2015 is listed below:

Computer Security Incidents in 2015	Number of Incidents	Percentage
Hacker Intrusion/ Web Defacement	151	3%
Phishing	1 978	40%
Botnet	1 943	39%
Distributed Denial-of-Service	130	3%
Malicious Software	277	6%
Others	449	9%
Total	**4 928**	**100%**

Category of Victims	Number of Incidents
Household and Individual	2 083
Large Enterprises and Organisations	146
Small and Medium Enterprises	374
Education Sector	109
Other Local and Overseas Internet Users	99
Unclassified (Internet users were unreachable directly)	2 117
Total	**4 928**

The HKCERT is mainly responsible for giving advice on incident response and system recovery to victims, who are not required to provide figures on their financial loss during the process.

Examination of Estimates of Expenditure 2016-17 Reply Serial No.

ITB198

CONTROLLING OFFICER'S REPLY

(Question Serial No.1946)

Head: (47) Government Secretariat : Office of the Government Chief Information Officer

Subhead (No. & title):

Programme: (1) Use of IT in Government
Controlling Officer: Government Chief Information Officer (Allen YEUNG)
Director of Bureau: Secretary for Innovation and Technology

Question:

Regarding the measures on promoting cyber and information security, please advise on the following:

(1) The number of cyber attacks (web defacement, intrusion of networking and information systems, and distributed denial of service (DDoS) attacks) targeting government networks and websites in 2015-16, broken down by department and type of security incidents in tabular form;

(2) The expenditure of government bureaux and departments (B/Ds) for security risk assessments and audits in 2015-16, and the percentage against their annual information technology (IT) expenditure;

(3) Have information security risk assessments and checks been performed for websites, applications and mobile applications developed by B/Ds in 2015-16? What are the details and expenditure involved?

(4) What are the estimated expenditure for the study and review on the government IT security policy, as well as the work, manpower and expenditure involved in 2016-17?

(5) Please list out in tabular form the B/Ds with IT security compliance monitoring and audits conducted in the past 3 years, being conducted and planned to be conducted in 2016-17; and

(6) Please list out in tabular form the dates, details, training departments, targets and numbers of participants of the security awareness seminars and training organised in the past 3 years, being organised and planned to be organised in 2016-17.

Asked by: Hon Charles Peter MOK (Member Question No. 9)

Reply:

The required information is provided as follows:

(1) In 2015-16, the Government Information Security Incident Response Office under the Government Computer Emergency Response Team (GovCERT) received 4 incident reports on cyber attacks targeting government websites, including 2 web defacements and 2 distributed denial of service attacks, which involved 4 different departments. No data leakage was found in the 4 security incidents.

(2) Government bureaux and departments (B/Ds) will conduct security risk assessments before launching new information systems or large-scale upgrade of the existing systems, and they are also required to perform regular security audits on information systems to ensure compliance with IT security policies and the implementation of effective security measures. The expenditure of such work is generally included in the development and maintenance costs of the relevant information systems. Therefore, we do not have a separate breakdown for the expenditure.

Besides, B/Ds conduct comprehensive information security risk assessments and audits periodically (around once every 2 years). In 2015-16, the estimated total expenditure on security risk assessments and audits was about $12.1 million, accounting for about 0.26% of the estimated total annual IT expenditure.

(3) It is a mandatory requirement to conduct information security risk assessments on websites, application systems and mobile applications developed by B/Ds. The risk assessments are generally included in the development and maintenance requirements of the relevant information systems. As the expenditure on information security is usually included in other IT-related expenditure, we do not have a separate breakdown for the expenditure in this regard.

(4) We have engaged a consultant to conduct the study and review on the government IT security policy. The estimated total expenditure is $3 million.

(5) The numbers of B/Ds with information security compliance audits conducted in the past 3 years, being conducted and planned to be conducted in 2016-17 are tabulated as follows:

Information Security Compliance Audit	2013-14 (Number of B/Ds)	2014-15 (Number of B/Ds)	2015-16 (Number of B/Ds)	2016-17 (Number of B/Ds)
Completed	8	8	25	-
Being conducted	-	-	2	-
Planned to be conducted	-	-	-	18

(6) The numbers of seminars and training organised in the past 3 years are tabulated as follows:

	2013-14	2014-15	2015-16
Number of seminars and training	48	65	53
Number of participants	1 342	2 213	1 617

These seminars and training included information security awareness training arranged for B/Ds' staff, information security refresher courses for departmental information security officers and commanders of departmental information security incident response teams, as well as thematic seminars and professional training for information security management and professional officers.

In 2016-17, we will continue to arrange relevant seminars and training. Detailed information is not available at the moment.

- End -

Examination of Estimates of Expenditure 2016-17 Reply Serial No.

ITB238

CONTROLLING OFFICER'S REPLY

(Question Serial No. 5037)

Head: (47) Government Secretariat : Office of the Government Chief Information Officer

Subhead (No. & title):

Programme: (1) Use of IT in Government
Controlling Officer: Government Chief Information Officer (Allen YEUNG)
Director of Bureau: Secretary for Innovation and Technology

Question:

Regarding matters on conducting security checking for government websites and web applications, will the Government inform this Committee of the following:

a) What is the expenditure on the related security checking? Are there any results and conclusion achieved? If yes, what are the details? How does the Government handle and respond to the results of such checking, and strengthen its internal capabilities in protecting its information systems? If not, what are the reasons?

b) Will the Government continue to strengthen its internal capabilities in protecting its information systems in 2016-17? If yes, what are the details? What is the expenditure involved? If not, what are the reasons?

Asked by: Hon SIN Chung-kai (Member Question No. 46)
Reply:

The required information is provided as follows:

a) The security checking is conducted through redeployment of resources and no additional resources are involved. The results revealed that government bureaux and departments (B/Ds) have implemented effective information security measures to guard against cyber attacks. Besides, B/Ds will also conduct security risk assessments periodically and enhance the protection capabilities of their information systems in a timely manner.

b) In 2016-17, the Office of the Government Chief Information Officer (OGCIO) will complete the review on the prevailing "Government IT Security Policy and Guidelines" to strengthen the compliance requirements and security practices, in order

to address different types of emerging threats. The estimated expenditure for the review is about $3 million. In addition, OGCIO plans to establish a cyber threat information sharing platform in 2017 to collect and analyse information on cyber security vulnerabilities and threats from various sources, and disseminate timely warnings and provide recommendations of responses to protect government information systems. The estimated expenditure for the project is about $6 million. B/Ds will also enhance the protection capabilities of their own information systems according to their respective risk levels and cyber threats. We do not have a breakdown for the estimated expenditure of B/Ds in this regard in 2016-17.

- End -