CB(1)1097/05-06(01)

For Information
on 17 March 2006

Legislative Council Panel on Information Technology and Broadcasting

Information Security

Purpose

This paper informs Members about the present play of information security in the wake of the recent information leakage on the Internet as reported in the media.

Government's Posture on Information Security

2. Government places great emphasis on information security and the protection of its information and computer assets. Under the Digital 21 Strategy for information and communications technology (ICT) development, establishing a secure environment is one of the key enablers in the promotion and development of ICT in Hong Kong. Various initiatives on information security have been launched to help promote the public confidence in conducting electronic transactions which in turn facilitate e-government and e-commerce to flourish. Over the years, we have made substantial progress on a number of information security related initiatives to develop a public information security infrastructure to facilitate e-business.

3. Government has also led by example in adopting international best practices and standards in protecting its information systems. It also reaches out to the business and general community using different channels to promote awareness of and educate the public in information security.

Hong Kong's Legal Framework Relevant to Information Security

4. Hong Kong maintains a comprehensive legal framework to protect against and deal with computer related crime and misuse of personal information. This includes -

(a) Crimes Ordinance (Cap. 200) - extending the meaning of property to include any program or data held in a computer; extending the meaning of criminal damage to property to misuse of a computer program or data;

(b) Telecommunications Ordinance (Cap. 106) - prohibiting unauthorized access to computer by telecommunication;

(c) Theft Ordinance (Cap. 210) - extending the meaning of burglary to include unlawfully causing a computer to function other than as it has been established and altering, erasing or adding any computer program or data; extending the meaning of false accounting to include destroying, defacing, concealing or falsifying records kept by computer;

(d) Personal Data (Privacy) Ordinance (Cap. 486) - protecting the privacy of living individuals in relation to personal data; applies to any person (data user) that controls the collection, holding, processing or use of personal data, including those in electronic form;

(e) Patents Ordinance (Cap. 514) & Trade Marks Ordinance (Cap. 43) - providing comprehensive protection for recognized categories of literary, dramatic, musical and artistic works, as well as for films, television broadcasts and cable diffusion, and works made available to the public on the Internet; and

(f) Electronic Transactions Ordinance (ETO) (Cap. 553) - providing a clear legal framework for the conduct of e-business in Hong Kong; according electronic record and electronic signature the same legal status as that of their paper-based counterparts, and establishing a voluntary recognition scheme for certification authorities (CA) and digital certificates that they issue, to enhance public confidence in electronic transactions.

5. In order to contain the problem of unsolicited electronic messages, an Unsolicited Electronic Messages Bill is in drafting and will be submitted to the legislature later in 2006.

Public Information Security Infrastructure

6. Apart from the legal framework, Hong Kong’s information security infrastructure comprises a number of important components. In

2000, the Office of the Government Chief Information Officer (OGCIO)[1] established the Certification Authority Recognition Office to support the voluntary recognition scheme for certification authorities and digital certificates under the ETO. This led to a public key infrastructure of technical mechanisms, procedures and policies that collectively provide a framework for addressing the requirements of confidentiality, authenticity, integrity and non-repudiation in electronic transactions.

7. In 2001, Government provided funding to set up the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) under the Hong Kong Productivity Council. The objective of HKCERT is to provide a centralized contact on computer and network incident reporting and response for local enterprises and Internet users in case of security incidents. It provides advice on preventive measures against security threats and organizes awareness seminars and training courses on information security related topics.

8. Since June 2003, the Immigration Department has been issuing the Multi-Application Smart ID Card to all Hong Kong citizens, with an option to include a recognized digital certificate. This community infrastructure enables business sectors, public organizations and government departments to explore opportunities for delivering electronic services in a secure manner on a common and convenient platform.

9. In mid-2005, the Hong Kong Monetary Authority and the Hong Kong Association of Banks announced the requirement of two-factor authentication for high-risk retail Internet banking transactions. This form of authentication uses a combination of 2 different factors for verifying a user's identity e.g. digital certificate, token-based one-time password and SMS-based one-time password.

The Government’s Internal Information Security Framework

10. Government has developed a comprehensive set of information security policy and guidelines for use by bureaux and departments (B/Ds). We have also implemented the management structure, technical security measures and other security mechanisms to monitor, detect and block suspected and potential attacks on the computer systems and networks.

Information Security Management Structure

[1] The OGCIO was set up in July 2004 by merging the IT-related divisions of the Commerce, Industry and Technology Bureau with the Information Technology Services Department (ITSD).

11. The OGCIO has developed and maintained comprehensive information technology (IT) security policies, procedures and relevant guidelines in addition to technical measures. These include a Baseline IT Security Policy, IT Security Guidelines, Security Risk Assessment and Audit Guidelines, and Information Security Incident Handling Guidelines. These procedures and guidelines were developed with reference to international best practices, professional sources and are reviewed from time to time to reflect changes in technology and security threats. They cover in considerable detail the organisational, management, technical and procedural aspects to enable B/Ds to build up their information security framework and practice. Examples of the topics covered by these guidelines are set out in the Annex. They are to be adopted by all B/Ds who are also required to comply with the Government's Security Regulations (SR). Among other things, the SR has a dedicated section covering information systems and related topics on the storage, processing and transmission of information, including classified information, cryptographic key management, physical security, and proper destruction of classified information.

12. To oversee and enforce information security within the Government, an Information Security Management Committee (ISMC) with core members from the Security Bureau and OGCIO was established in 2000. An IT Security Working Group (ITSWG) 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.

Security Threat Alerts and Incident Response

13. In addition to the central information security management structure, a Government Information Security Incident Response Office (GIRO) was set up in 2001 which co-ordinates and support all departments in the handling of Government information security incidents. To support the GIRO, a Standing Office in the OGCIO monitors round the clock computer virus and information security incidents, outbreaks or alarms from all sources globally, and reports to the relevant units in the security framework as and when necessary. Virus alerts and security reminders are issued to departments as soon as a security problem is identified and assessed to be serious. Administrators of major government infrastructure systems are required to submit weekly information reports to the OGCIO on the security status of their systems and other issues relating to IT security for management monitoring and control purposes.

14. At the departmental level, there are also management structures

to implement various security measures to protect Government's information systems. All departments are required to appoint a senior officer to be the Departmental IT Security Officer (DITSO) who is charged with the responsibility for the overall information security management and operation of the department. In addition, an Information Security Incident Response Team (ISIRT) is set up in every department to deal with all matters on a day-to-day basis relating to security incident reporting and response. Depending on the size of the department and the nature and complexity of its business, the staffing arrangements for the DITSO and the ISIRT may vary.

Information Security Protection Measures and Approach

15. Government adopts the principle of 'protect, detect, react and respond' and implements necessary measures in ensuring the integrity of business transactions and information by guarding against various types of cyber attacks such as computer worms and viruses, hacking, spamming and computer crimes. Deploying state-of-the-art technology, we use firewalls, anti-virus software, intrusion detection systems and other defensive mechanisms to monitor, detect and block suspected and potential attacks on our computer networks and systems which are kept up-to-date by applying the necessary patches and fixes regularly.

16. Government also performs regular security reviews and audits of the technical and procedural measures to ensure that they can keep up with technology advancements and industry best practices, and changes in the system, network, or organizational environment. The OGCIO has put in place standing offer agreements for information security professional services to facilitate B/Ds who need to engage external resources to develop security policies, procedures and to perform security reviews and audits of their systems. Between 2002 and 2005, B/Ds have engaged some 140 service assignments of this nature under the centrally organized contracts, with a total expenditure of some $45 million.

Overall Information Security Status in Government

17. Government has been adopting IT in its business and delivery of public services aggressively over the past few years. The information security framework and resources deployed have also shown corresponding growth and enhancement. Our efforts in maintaining a comprehensive information security posture have been producing encouraging results. Based on reports received by the GIRO, the number of cases of information security incidents has been maintained at a relatively low level and on the

decrease over the last five years. For example, the number of substantiated incidents has decreased from 9 in 2002 to 3 in 2005, with no loss of data/information involved. This can be attributed to the increasing management attention and rigorous compliance with the established security policies and guidelines by B/Ds. In the run up to the Sixth Ministerial Conference of the World Trade Organisation held in Hong Kong in December last year, we have further enhanced the information security provisions in B/Ds. As a result, no security related incident was reported during the conference period. We are of course not complacent about this and will continue to uphold a high level of security protection in our systems and data.

Government Measures on Information Security Targeted at the Community

18. Government is committed to making Hong Kong a leading e-business community and digital city. Information security is an important pillar to support the fast pace with which our e-business needs to develop.

Industry Support and Liaison

19. Government encourages the industry, the academia and related bodies to conduct research and development to enable knowledge-based society to flourish, and has been providing funding support where applicable. The Police has established facilities and developed expertise in technology crimes, including computer forensics, which has enabled the successful crack down of some cyber crime cases in recent years. The setting up of the HKCERT in 2001 has enhanced Hong Kong's information security incident response capability. In 2005, the OGCIO also set up the Internet Infrastructure Liaison Group (IILG)[2] to facilitate local Internet stakeholders to share information and deal with incidents relating to the Internet in a coordinated way. It also established a Special Task Force on Information Security comprising OGCIO, Police, Education and Manpower Bureau, interested members of the Digital 21 Strategy Advisory Committee, and representatives from information security industry associations to look into specific issues that help to enhance Hong Kong's overall information security standing.

Public Awareness and Education on Information Security

20. In 2002, the OGCIO set up the INFOSEC web site at

[2] IILG members include the Hong Kong Internet Exchange (HKIX), the Hong Kong Domain Name Registration (HKDNR), HKCERT, Hong Kong ISP Association, the Police, OFTA and OGCIO.

"www.infosec.gov.hk" to provide a one-stop portal to facilitate public access to various information security related resources and updates. We have also published on the website international best practices and standards widely adopted in countries advanced in IT. In addition, the OGCIO has also periodically produced radio episodes and TV features to raise the awareness of, promote ethical practices, and educate and update the public on prevention of computer crime and contemporary information security issues such as spamming. Information leaflets are distributed through various channels including community facilities, libraries and schools, and during various events such as exhibitions, conferences and seminars.

21. In 2003, the Security Bureau issued an information paper to local professional organizations and business associations to share with them information and updates on international information security standards and to invite their consideration of formulating their sector specific information security standards and audit mechanisms which could recognize the characteristics of different industries.

22. At the regional level, OGCIO is a member of the APEC Telecommunications and Information (TEL) Working Group which is focusing more and more on e-commerce, digital divide and its related issues especially in IT security and computer emergency response. OGCIO is an active participant in the APEC TEL and its related developments in information security. Through this, we aim to increase Government's capacity in intelligence collection, information exchange and response to potential outbreaks of major information security incidents in the region.

Planned Activities for 2006-07

23. Information security continues to be one of the major work areas of the Government. We will continue to take forward a number of initiatives within Government and in the wider community to enhance their awareness and preparedness to deal with information security issues.

Within Government

24. In 2006-07, the OGCIO will be –

(a) Updating the information security regulations, policies and guidelines within the second quarter of 2006 to keep them in pace with the advancement of technology and the development of international/industry practices;

(b) Strengthening the cyber security management, monitoring, threats alert and incidents response mechanisms among B/Ds and in collaboration with relevant parties such as the Police, the HKCERT and other Internet infrastructure stakeholders;

(c) Keeping abreast of current knowledge and research material on information security and related technology; publishing guidelines on proactive preventative actions for reference by B/Ds; and

(d) Organising training and seminars for B/Ds at both management and technical levels on contemporary information security issues and relevant international best practices such as anti-spamming and standards adoption.

25. The estimated expenditure for 2006-07 for these activities is $1.3 million. This expenditure does not include resources for conducting security reviews and audits in other B/Ds, which will be funded through their respective departmental expenditure envelopes or the Capital Works Reserve Fund (CWRF) Head 710 Computerisation, depending on the scope and size of the project.

In the Community

26. In 2006-07, we will continue the promotion of and public education on the wider use of IT and information security in the community -

(a) We will increase the efforts on the promotion of IT awareness to and adoption by disadvantaged groups and the small and medium sized enterprises (SMEs) in various business sectors. Of equal importance in the use of IT, we will continue to upkeep the general public on contemporary knowledge and issues on information security such as best practices in preventing and tackling computer crimes, e-business frauds and spamming as well as the adoption of relevant international standards by enterprises in protecting their information assets.

(b) In addition, we will continue to provide relevant reference material and expert advice in the one-stop INFOSEC website for public reference. In collaboration with the industry, we will organise exhibitions and seminars on themes such as anti-spamming that are of public interest. We will explore with professional associations and relevant organisations to arrange short training classes for the public aiming to enhancing their information security awareness. We will produce a new series of radio programmes to educate the public on information asset protection and computer crime prevention.

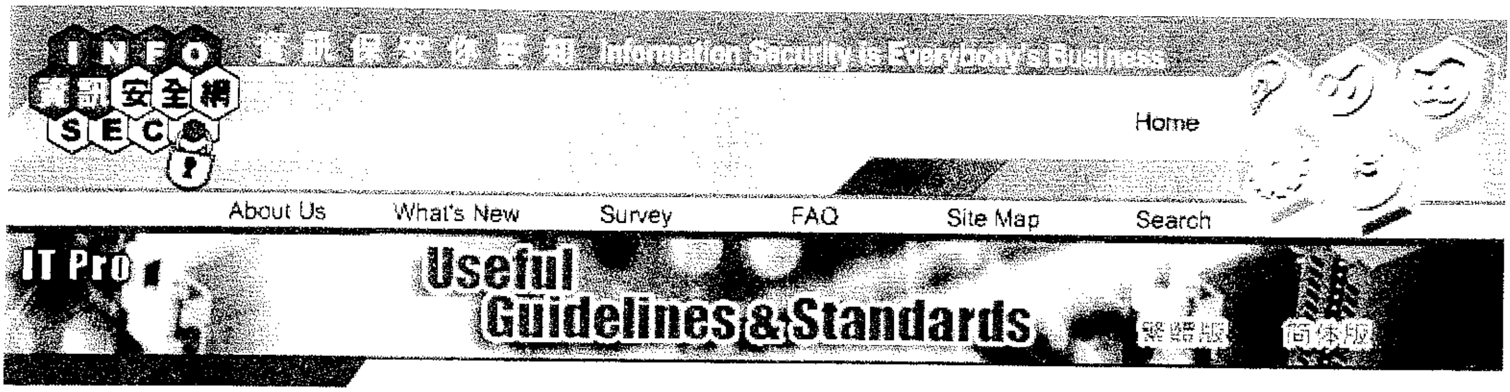
27. The estimated expenditure for information security promotion targeted at the community is $1 million.

Advice Sought

28. Members are invited to note the comments of this paper.

Office of the Government Chief Information Officer
Commerce, Industry and Technology Bureau
March 2006

Annex


INFO
資訊安全網
SEC
資訊保安你要知 Information Security is Everybody's Business
Home
About Us
What's New
Survey
FAQ
Site Map
Search
IT Pro
Useful Guidelines & Standards
繁體版
简体版

- IT Pro Corner
- Security Tips
- Technical References
- Useful Guidelines & Standards
- Security Management
- Related Ordinances
- Public Services
- Computer Virus
- News & Events
- Glossary
- Download
- Useful Links

To facilitate your planning on information security management for your company, we have highlighted some useful guidelines that are recommended as effective security practices and internationally recognized standards related to information security.

- **IT Security Policy and Guidelines**
- **Standards for Information Security**
- **IT Security References**

(To view and print the downloaded document, you need to use an Adobe Acrobat Reader. Please click here to download if necessary. Adobe Get Acrobat Reader)

IT Security Policy and Guidelines

The Government of HKSAR has issued a Baseline IT Security Policy and a series of guidelines related to IT security to provide references and guidance to Government bureaux and departments in respect of the protection of Government information systems. The related documents are obtainable through the hyperlinks provided below. Users should note that the documents are for general reference only and users are responsible to make their own assessment on the information provided and to obtain independent advice before acting on it.

- **Baseline IT Security Policy** - This document sets the baseline standards of IT security policy for Government bureaux/departments. It states what aspects are of paramount importance.

- **IT Security Guidelines** - This document introduces concepts relating to IT security and elaborates further on the Baseline IT Security Policy.

- **Internet Gateway Security Guidelines** - This document acts as a supplementary document to IT Security Guidelines to provide guidelines on Internet gateway security.

- **Security Risk Assessment & Audit Guidelines** - This document acts as a supplementary document to IT Security Guidelines to give an introduction to a generic reference model for IT security risk assessment and security audit.

- **Information Security Incident Handling Guidelines** - This document acts as a supplementary document to IT Security Guidelines to provide reference for the planning and preparation for, the detection of, and the response to information security incidents.

- Top -

Standards for Information Security

- **ISO 17799 -** A code of practice for information security management.
- **ISO 7498, Open System Interconnection Model** - ISO/IEC 7498 Security Architecture, part 2 (superceded by ISO/IEC 10745 and ITU-T X.803 "Upper Layers Security Model", ISO/IEC 13594 and ITU-T X.802 "Lower Layers Security Model", and ISO/IEC 10181-1 and ITU-T X.810 "Security Frameworks, Part 1: Overview").
- **British Standard 7799** - A business-led approach to best practice on information security management.
- **Trusted Computer System Evaluation Criteria (TCSEC) or called the Orange Book** - Classification on security requirements based on evaluation of functionality, effectiveness and assurance of mostly operating systems for mainly government and military sectors. TCSEC was introduced in 1985 and retired in 2000.
- **The Rainbow Series** - A series of books that extend the coverage of the Orange Book into other areas of security. Example is:
    - Trusted Network Interpretation (TNI) or called the Red Book -provides a framework for securing different types of networks and network components.
- **Information Technology Security Evaluation Criteria (ITSEC)** - the first single standard for evaluating security attributes of computer systems by European countries and used only in Europe.
- **Common Criteria** - combine and align existing and emerging evaluation criteria with a collaborative effort among national security standards organizations of Canada, France, Germany, the Netherlands, the UK and the US.
URL://csrc.nist.gov/cc/Documents/CC%20v2.1%20-%20HTML/CCCOVER.HTM

- Top -

IT Security References

- **Establishing a Computer Security Incident Response Capability**, NIST (National Institute of Standards and Technology) Special Publication 800-3, Nov 1991.
- **Sample Incident Handling Procedures**, from SANS (System Administration, Networking, and Security Institute), April 1998.
- **RFC 2196 Site Security Handbook**, from IETF (The Internet Engineering Task Force).
- **RFC 2350 Expectations for Computer Security Incident Response**, from IETF (The Internet Engineering Task Force).
- **Responding to Computer Security Incidents: Guidelines for Incident Handling**, University of California Lawrence Livermore National Laboratory, July 1990.
[Source: The U.S. Department of Energy's Computer Incident Advisory Capability (CIAC)]
- **SANS/FBI Top 20 Most Critical Internet Security Vulnerabilities List**

The list includes 20 vulnerabilities organized into 3 categories: vulnerabilities that affect all systems, those that affect Windows systems, and those that affect Unix systems.

- **ISACA's Standards, Guidelines and Procedures**
  The Information Systems Audit and Control Association issues a series of information systems auditing standards, guidelines and procedures.

- Top -

Last update / review: March 2006

Disclaimer

The Office of the
Government Chief Information Officer

BASELINE IT SECURITY POLICY

[S17]

Version : 2.3

Nov 2004
The Government of the Hong Kong Special Administrative Region

TABLE OF CONTENTS

The Office of the
Government Chief Information Officer

IT SECURITY GUIDELINES

[G3]

Version : 4.3

Nov 2004
The Government of the Hong Kong Special Administrative Region

TABLE OF CONTENTS

APPENDIX

The Office of the
Government Chief Information Officer

SECURITY RISK ASSESSMENT & AUDIT GUIDELINES

[G51]

Version : 2.1

Jul 2004
The Government of the Hong Kong Special Administrative Region

TABLE OF CONTENTS

APPENDIX

The Office of the
Government Chief Information Officer

INFORMATION SECURITY INCIDENT HANDLING GUIDELINES

[G54]

Version: 2.2

Sep 2004
The Government of the Hong Kong Special Administrative Region

TABLE OF CONTENTS

APPENDIX