LC Paper No. CB(1)435/06-07(05)

For Information
on 11 December 2006

Legislative Council Panel on
Information Technology and Broadcasting

Information Security

A. Purpose

This paper informs Members about the information security status of public organizations and the various initiatives that are pursued by the Government in strengthening the information security protection measures.

B. Background

2. The Government presented an information paper on information security (LC Paper No. CB(1)1097/05-06(01)) to the LegCo Panel on Information Technology and Broadcasting (ITB Panel) on 17 March 2006, describing the measures taken by the Government in protecting the information assets and personal data kept by Government bureaux and departments (B/Ds). While these measures are being pursued, the rapid advancement in information and communications technologies (ICT), hence the associated cyber security threats have necessitated that our level of protection must be geared up to the pace of such developments.

C. Report on the Information Security Status of B/Ds, Public Organizations and Regulatory Bodies

3. On the request of the LegCo ITB Panel in its meeting held on 6 April 2006, the Government has conducted a survey on the information security status of Government B/Ds, public organizations and how regulators monitor the information security compliance of organizations under their purview. The findings of the survey are reported in **Annex A** of this paper.

D. Proposed Follow-up Actions

4. In view of recent information security incidents and drawing from findings derived from the survey, the Government has included additional initiatives to the overall information security programme that will strengthen the protection measures for Hong Kong. The following sections describe the latest progress and planned enhancements of the various protection measures.

(i) Measures Targeted at Government B/Ds

5. The Government will continue to lead by example in the adoption of ICT, as well as ensure a strong information security profile of its B/Ds.

Policy and Governance

6. The Government will continue to review and enhance the information security related regulations, policies, procedures and guidelines to keep them in pace with the advancement of technology, the development of international/industry best practices and standards and the emerging security threats. A recent review exercise was completed in May 2006 and the changes were promulgated to the B/Ds for adoption.

Assurance and Compliance

7. The Government Chief Information Officer (GCIO) has reminded Heads of B/Ds that information security risk assessment, assurance and audits should be conducted regularly and at least biennially on critical information systems. The most recent reminder was issued in early October 2006. We will also introduce an additional mechanism that requires B/Ds to submit annual reports on their compliance with government information security requirements. These reports will be required to be endorsed by the senior management of the B/Ds.

Tender Requirements in IT Outsourcing

8. The OGCIO has built in contractual provisions in the centrally managed contracts to ensure that outsourcing contractors and their sub-contractors of IT and related services are contractually required to follow the information security requirement similar to Government staff. We have also reminded B/Ds to have similar provisions for services procured on their own arrangement.

9. We will remind B/Ds to exercise extreme discretion in drawing up procurement specifications in IT outsourcing in order to ensure software quality of systems that handle personal and classified data in accordance with the government information security requirements. B/Ds when approving outsourcing arrangements should indicate explicitly that government information security requirements including outsourcing security, physical security, access control security, data security, application security, network and communication security as stated in the Baseline IT Security Policy have been considered and included in the procurement specification.

Independent Security Audits

10. The onus of information security requirement compliance checking continues to rest with the B/Ds because they know their business well. To enhance the effectiveness of security compliance checking of B/Ds, the Government will introduce a centrally managed process in the form of security audits to conduct random/sample checks in order to confirm that the necessary security risk assessments and reviews have been satisfactorily performed and any recommendations for improvement are properly dealt with. We plan to start this audit process in early 2007 and, over a 2-year period, cover all B/Ds.

Staff Awareness and Education

11. The OGCIO has issued circulars on information security matters and regularly reminders to B/Ds to draw their attention to emerging software vulnerabilities, security threat alert notices and also tips and techniques in combating security incidents. The GCIO has

reminded Heads of B/Ds to ensure that information security and related circulars, information notices and security alerts are circulated to all staff. B/Ds are also advised to periodically re-circulate these documents to maintain maximum staff awareness. In order to facilitate government staff to build up their security awareness and knowledge, we will study and provide the use of multiple channels to deliver training materials on general security awareness and data protection so that they can acquire such knowledge at any time and through means more flexible and accessible to them.

(ii) Measures Targeted at Public Organizations

12. The survey findings on information security status of public organizations have identified urgent need for improvement especially in some organizations. Naturally, organizations that fall short in key security aspects are more vulnerable to security attacks, information exposure or data loss. To enhance the information security status of public organizations, the OGCIO will advise the responsible B/Ds to follow up on the security protection improvement and the exposures represented by the status quo of the organizations under their purview pursuant to the findings from the survey.

(iii) Measures Targeted at Regulated Bodies/Sectors

13. Information security incidents, e.g. the leakage of personal data involving any organizations may have serious impacts across their sectors such as their trustworthiness or lead to possible legal proceedings. The OGCIO will remind the B/Ds that have purview over regulatory bodies about the importance of putting in place the necessary information security measures by organizations within their regulated sectors. The regulatory bodies should consider tightening the regulatory regime to emphasize the importance of information security and protection of personal data. The public awareness and education programmes as described in the ensuing paragraphs are also relevant to these organizations.

(iv) Measures Targeted at General Public

Personal Data Privacy Protection

14. To address the growing concerns in the community about data privacy relating to electronic communications and transactions, we will cooperate with the Privacy Commissioner's Office and relevant industry bodies in promoting the importance of personal data privacy protection. We will also extend our existing effort in convening conferences, seminars and exhibitions for the industry and relevant practitioners to share best practices and experience on data protection.

Promotion and Education to the Community

15. The OGCIO employs a variety of information dissemination channels for the launch of activities in information security promotion and education. The one-stop information security portal (http://www.infosec.gov.hk) provides the latest news, up-to-date reference information and security alerts accessible by the public. We will continue to enrich the contents of the website, notwithstanding that we have enhanced the number of theme pages from 1,200 to 1,400 within 2006. We are also launching a series of promotional activities as shown in **Annex B**. These include enhancing the resources available for public reference through website, seminars, conferences, radio programmes, TV episodes, publicity leaflets and a carnival.

16. To facilitate the adoption of proper access control as the gate-keeping mechanism when using electronic services in business transactions or private communications, the Government will publish a guideline on security risk assessment and electronic authentication in 2007/08. This will enable the electronic service providers and users determine the appropriate authentication requirements during electronic exchanges.

Collaboration with industry players

17. The OGCIO is collaborating with the Hong Kong Police Force (HKPF) and the Hong Kong Computer Emergency Response Team

Coordination Centre (HKCERT) to launch the “Hong Kong Clean PC Day 2006” Campaign in November 2006 to raise public awareness on information security and strengthen the protection of their computers from cyber attacks by adopting easy techniques.

18. The OGCIO will continue its regional and international levels of collaboration with the Asia Pacific Computer Emergency Response Teams (APCERT), Forum of Incident Response and Security Teams (FIRST), APEC Telecommunications and Information (TEL) Working Group to increase the Government’s capability in intelligence collection, information exchange and response to potential outbreaks of major information security incidents.

E. Conclusion

19. Information Security management is an ongoing process and requires the commitment and attention of everyone. The Government will continue to enhance the security measures in B/Ds and advise the public organizations and the regulatory bodies on how to improve their information security status through the B/Ds having purview over them. Under the Government’s Digital 21 Strategy, we will continue to promote public awareness and knowledge about information security and data privacy. This will contribute to making Hong Kong a more secure digital city for the conduct of e-Commerce.

F. Advice Sought

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

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

Annex A

Report on Information Security Status of Government B/Ds, Public Organizations and Regulatory Bodies

This Annex reports on the survey findings on information security status of government bureaux and departments (B/Ds), public organizations and regulatory bodies.

A. Background

2. At the LegCo Panel on Information Technology and Broadcasting (ITB Panel) meeting held on 6 April 2006, the Administration was requested to provide a comprehensive report on the current state of information security in B/Ds as well as how various regulators exercise their monitoring role to ensure that information security is being observed and complied with by the relevant sectors under their purviews. Furthermore, the Administration was also requested to collect information from public organizations on the measures taken by them to maintain and enhance information security.

B. Survey Methodology

3. Two surveys have been conducted to collect the data required for compiling this report. The survey on B/Ds is an annual exercise conducted by the OGCIO in July 2006 to ascertain the overall security status of the government. For the other survey, B/Ds having purview over their public organizations and regulatory bodies were asked to coordinate the completion and return of the survey questionnaires in August this year.

4. Each group of the surveyed organizations uses a different set of questionnaire that suits their characteristics. All the returns have been verified for completeness, and where required with clarifications or supplementary input collected. The data of each group are then collated, analyzed and aggregated for compiling the findings in this report.

C. Information Security Status

<u>Government B/Ds</u>

5. The analysis in this part is based on data collected from the 84 (out of 84) B/Ds. The findings cover mainly the aspects of security management and governance, protection measures in handling restricted/classified data, IT services outsourcing and adoption of technology measures for protection. The following are the major findings.

(i) Security Management and Governance

6. The government has established information security policy and management framework at the centre and within individual B/Ds. There are information security related regulations, policies, procedures and guidelines in place for the compliance of B/Ds. There are also clear formulation of roles and responsibilities on security governance and control.

7. About 84% of B/Ds have completed their scheduled IT security risk assessment and audit. The rest will also complete the exercise within this financial year. All B/Ds that have implemented mission critical systems have contingency measures in the form of business continuity plan and/or disaster recovery plan to handle cyber security incidents.

(ii) Handling of Restricted/Classified Data

8. Most B/Ds handle personal/classified data which they have implemented security measures for protection. These measures include applying data encryption, exercising access controls during IT application development, system maintenance and operation work, and properly labeling and keeping safe of the classified data and their physical storage media.

(iii) Arrangement in IT Outsourcing

9. About 80% of B/Ds have acquired IT outsourcing services and they have incorporated various security measures and monitoring controls in the procurement contracts. Over 90% of these contracts contain the necessary information security requirements that the contractor staff have to observe. Centrally managed contracts contain the necessary provisions to ensure that the contractors and their sub-contractors comply with the government's information security requirements.

(iv) Technology Measures

10. All B/Ds apply patch management to ensure that software vulnerabilities are properly fixed. Over 70% have automated the process to ensure the timely application of software patches to secure their IT systems.

(v) Staff Awareness, Education and Training

11. Information security awareness programmes and training courses are centrally organized by the OGCIO for government staff. To cater for departmental needs, 29% have organized other in-house awareness promotion and tailor-made training for their staff.

Public Organizations

12. This part covers data collected from the 104 (out of 104) public organizations (full list in **Enclosure 1** of this Annex). The findings cover general information, security management and governance, protection measures in handling restricted/classified data, IT services outsourcing, adoption of technology measures for protection and staff awareness and education towards information security.

(i) General Information

13. The overview of organization size, extent of use of IT and trend of expenditures on information security are provided below in Tables 1, 2 and 3 respectively.

Table 1 – Organization Size (According to The Number of People Working On-site)

45%	Small (1-9 staff)
20%	Medium (10-99 staff)
35%	Large (>99 staff)

Table 2 – Adoption of IT (Office/Operation Automation or IT/Business Integration)

4%	Employing leading edge IT applications
94%	Normal user of IT
2%	Only getting started

Table 3 – Expenditure Trends on Information Security

12%	Increased from last financial year
84%	No change
4%	Decreased from last financial year

14. The number of personal computers (PCs) used is roughly proportional to the size of the organizations. These PCs are generally connected to the Internet, hence are potentially subject to cyber attacks. Half of the respondents consider that IT service failure including information security incidents will affect their business operation. About 30% consider that IT failure will also have high impact to their internal administration.

(ii) Security Management

15. The public organizations have been asked whether they have adopted any of the measures for security management. The findings and observations are described in Table 4 and paragraphs 16-17 below.

Table 4 – Security Management Measures Adopted by Public Organizations

Category of Management Measures	**Findings and Observations**
Policy/Management Governance	93% of the respondents have adopted at least one form of policy/management governance measures. The adoption of individual measures are- - management framework (60%) - policy or guidelines (59%) - requirement to comply with laws and/or regulations (78%)
Operational Protection Measures	All respondents have implemented at least one form of operational protection measures. The adoption of individual measures are- - security patch management (88%) - anti-virus management (100%)
Contingency Handling	72% of the respondents have implemented at least one form of contingency handling measures. The adoption of individual measures are- - incident and response management (61%) - business continuity management (63%)
Staff Awareness and Training	19% of the respondents mandate staff awareness and training programme
Security Risk Assessment and Audit	59% of the respondents adopt security risk assessment and audit

16. The findings above show that 40% have not established an information security management framework and 41% do not have information security policies or guidelines. On the operational side, 12% have not implemented security patch management to protect them from possible cyber attacks.

17. It is found that only 19% mandate staff awareness and training programme on information security, which is seriously inadequate. As many as 41% have not adopted any kind of security risk assessment and audit for information security assurance, and 34% of them have no such plan for the near future.

(iii) Governance of Security Implementation and Practices

18. The public organizations are asked how they ensure that the security management measures have been properly implemented and practised. The findings and observations are described in Table 5 below.

Table 5 – Security Governance Measures Adopted by Public Organizations

Category of Governance Mechanism	**Findings and Observations**
Test of Compliance	67% of the respondents have applied at least one measure to test security compliance. The adoption of individual measures are- - regular review (65%) - security incident/recovery drill (37%)
Supportive and Random Checks	69% of the respondents have implemented at least one form of supportive and random checks. The adoption of individual measures are- - internal auditing (50%) - surprise checks (16%) - business continuity procedures (50%)
Advice or Encouragement	93% of the respondents have employed at least one mechanism to serve as advice or encouragement. The adoption of individual measures are- - reminder/circular (88%) - criteria in approving funding (31%) - aspect of staff performance appraisal (19%)

(iv) Handling of Restricted/Classified Data

19. Over 85% of the respondents are required to handle restricted/classified data. The common data items include name, address, HKID number and phone number. A few also involve credit card number and bank account name.

20. The public organizations are asked whether they have adopted operational measures and/or technical tools when handling restricted/classified data. The findings and observations are described in

Table 6 and paragraphs 21-22 below.

Table 6 – Measures/Tools Adopted by Public Organizations When Handling Restricted/Classified Data

Category of Measures and Tools	Findings and Observations
Operational Measures	89% of the respondents have established at least one form of operational measures. The adoption of individual measures are- - data definition (73%) - authorization definition (55%) - procedures for granting access (73%) - control procedures for staff access (63%) - inventory management and control (63%) - backup/recovery/disposal procedures (74%)
Technical Tools	57% have adopted technical tools such as cryptographic tools in handling restricted/classified data during storage/transmission/processing.

21. The above findings show that proper authorization definition and access control procedures need to be strengthened in the handling of restricted/classified data. It is further noticed that 26% do not have backup, recovery and restricted/classified data disposal procedures.

22. On the prevention of restricted/classified data from unintentional disclosure, 43% do not utilize any technical tools such as cryptographic tools during their storage, transmission and processing of such data.

(v) Arrangement in IT Outsourcing

23. About 80% of the respondents have outsourcing arrangements to perform various IT work such as development, maintenance, operation, technical support, facility management and helpdesk. The findings and observations on security measures they have adopted in IT outsourcing are described in Table 7 and paragraphs 24-25 below.

Table 7 – Security Measures Adopted by Public Organizations in IT Outsourcing

Category of Security Measures	Findings and Observations
Contractual Provisions	93% of the respondents that have IT outsourcing arrangement have used at least one form of security measures in their contracts. The adoption of individual measures are- - non-disclosure agreement (80%) - service level agreement (69%) - stated requirement of access control, change control, escalation process, incident response (75%) - compliance statement (48%)
Quality Assurance and Control	75% of the respondents that have IT outsourcing arrangement have implemented at least one form of quality assurance and control measures. The adoption of individual measures are- - security control in different testing stages (66%) - quality assurance (53%)
Security Governance and Control	82% of the respondents that have IT outsourcing arrangement have put in place at least one form of security governance measures. The adoption of individual measures are- - security control on data (61%) - regular compliance check (45%) - formulation of roles and responsibilities (71%) - inventory control (57%)
Personnel Security Vetting	12% of the respondents that have IT outsourcing arrangement have performed personnel security vetting.

24. It is observed that security control applicable to testing stages is not adopted by as many as 34% of those public organizations that have IT outsourcing arrangement. The findings further show that 47% of them fall short of any quality assurance for their IT outsourcing arrangement and 39% without security control on the data.

25. In respect of governance, 29% have not formulated the roles and responsibilities with their outsource contractors, and more than half of them do not check contractor compliance against their information

security requirements.

(vi) Technology Measures

26. The findings and observations on the security technologies and tools that the public organizations use in protecting their computer data and facilities are described in Table 8 and paragraph 27 below.

Table 8 – Technology Measures/Tools Adopted by Public Organizations

Category of Technologies And Tools	**Findings and Observations**
Basic Measures	79% of the respondents have employed at least one form of the basic technical measures in protecting their computer data and facilities. The adoption of individual measures are- - user account with password (100%) - anti-virus utility (100%) - anti-spyware tool (45%) - security patch management tool (82%) - firewall (94%)
Special Data handling Measures	74% of the respondents have implemented at least one of the special data handling measures. The adoption of individual measures are- - file/data encryption (64%) - secure data removal tool (38%)
More Advanced Authentication/Access Control Technologies	77% of the respondents have implemented at least one of the more advanced authentication/access control technologies. The adoption of individual types are- - public key infrastructure (32%) - identity management (55%) - two or more factor authentication (25%) - audit logs and trailing tools (69%)

Table 8 – Technology Measures/Tools Adopted by Public Organizations (cont'd)

Category of Technologies And Tools	Findings and Observations
Network Related	88% of the respondents have employed at least one form of network related security measures. The adoption of individual types are- - email filtering tools (75%) - intrusion detection/prevention tool (52%) - secured network (59%)
Asset Protection	86% of the respondents have carried out at least one form of asset protection measures. The adoption of individual measures are- - physical security (70%) - backup recovery (85%)

27. The findings show that 18% of the public organizations still have not implemented security patch management tool suggesting that they are likely to be more vulnerable to cyber attacks. It is also found that 62% do not employ any secure data removal tool, 45% no identity management, 41% using unsecured network, and 30% without physical security measures to protect their computer assets.

(vii) Staff Awareness, Education and Training

28. On information security related awareness and education for staff, the findings and observations are described in Table 9 and paragraph 29 below.

Table 9 – Awareness and Training Programme Launched by Public Organizations

Category of Educational Measures	**Findings and Observations**
Facilitation	66% of the respondents use at least one of the facilitation measures to boost up information security awareness of their staff. The adoption of individual measures are- - internal training (39%) - external training (54%) - e-learning courses (13%)
Incentive for Staff to Acquire Information Security Qualification	11% of the respondents provide various incentives to encourage staff to acquire qualifications in information security skills.
Periodic Reminder	93% of the respondents issue reminders regularly to staff to alert them on information security and related matters.

29. The public organizations are also asked about the topics covered by the awareness and training programmes. About 7% reported that they provided a comprehensive range of the security topics including awareness, management, incident handling, outsourcing, technical techniques and skills and professional certification training.

Regulatory Bodies/Sectors

30. A total of 58 (out of 58) returns from regulatory bodies are received (full list in **Enclosure 2** of this Annex). Survey data of 13 sectors as returned by 11 regulatory bodies are obtained, and they form the basis of the findings in the following paragraphs. The rest practically provided nil returns as they considered that their sectors either did not have information security concerns or they did not specifically oversee information security of organizations in the sector.

(i) General Information

Table 10 – Sector Size Distribution (According to the Number of Organizations in the Regulated Sector)

46%	< 20 organizations
8%	150-199 organizations
23%	200-499 organizations
23%	>500 organizations

(ii) Regulatory Measures and Compliance Monitoring

31. The regulatory bodies are asked the information security measures that they use in regulating and monitoring organizations. The findings and observations are described in Table 11 and paragraph 32 below.

Table 11 – Regulatory and Monitoring measures adopted by Regulatory Bodies

Category of Regulatory And Monitoring Measures	**Findings and Observations**
Policy/Management	All regulatory bodies that have responded have at least one form of policy/management measures for monitoring the organizations under their purview. The adoption of individual measures are- - rules and regulations (100%) - mandatory information security management framework (15%)
Security Assurance	62% of the regulatory bodies that have responded require organizations in the sector to perform at least one form of security assurance measures. The adoption of individual measures are- - regular risk assessment/audit/review (38%) - report on major changes made to information systems (46%)

Table 11 – Regulatory and Monitoring measures adopted by Regulatory Bodies (cont'd)

Category of Regulatory And Monitoring Measures	**Findings and Observations**
Contingency Handling	69% of the regulatory bodies that have responded require organizations in the sector to put in place at least one form of contingency handling mechanisms. The adoption of individual mechanisms are- - information security incident procedures (69%) - business continuity planning (46%)
Staff Awareness and Training	54% of the regulatory bodies that have responded require organizations in the sector to provide staff with training on information security.

32. It is also reported that under the code of practice published by some regulatory bodies, organizations in the sector are required to establish approved policies and procedures to protect the data under their charge or purview. Some have established relevant industry associations for organizations in the sector to discuss precautionary measures and formulate guidance in respect of security incidents.

(iii) Protection of Restricted/Classified Data

33. Of the 13 regulated sectors, 92% handle restricted/classified data which include name, address, HKID number and phone number. A few of them also handle details about finance, contracts, business transactions and law amendment proposals.

34. Regarding the security measures that organizations in the sector adopt in protecting personal or restricted/classified data, the findings and observations are described in Table 12 and paragraph 35 below.

Table 12 – Security measures adopted by Organizations in the Regulated Sectors

Category of Security Measures	Findings and Observations
Policy/Management	85% of the regulated sectors have one least one policy/management measure in place. The adoption of individual measures are- - management and governance which include security policy, regulations, standards, guidelines and best practices (85%) - security process controls and procedures (77%)
Technical Measures	77% of the regulated sectors have employed technical measures which include data encryption, authentication means, intrusion detection and prevention system and logging.
Security Assurance	54% of the regulated sectors have implemented security risk assessment/audit/review.
Contingency Handling	69% of the regulated sectors have implemented at least one form of contingency handling measures. The adoption of individual measures are- - information security incident management (62%) - business continuity planning (69%)
Staff Awareness and Training	69% of the regulated sectors have arranged awareness and training programmes for their staff.

35. About 70% of the regulatory bodies have responded that they are satisfied with the implementation of information security protection measures by the organizations in the sectors. They also consider their monitoring measures adequate and effective.

D. Conclusion

36. The findings from the surveys on the 3 types of public organizations have revealed their information security status.

37. For Government B/Ds, as there are comprehensive management framework and well-established policy and guidelines promulgated from the center, B/Ds are expected to ensure their compliance with the

stringent government information security requirements.

38. There is urgent need for improvement in some public organizations and the regulatory bodies/sectors as revealed from the survey findings. As a high percentage of these organizations need to handle personal or restricted data, some of them should urgently enhance their management, governance, technology or procedural measures on information security in order to forestall incidents including data leakage. The exposures represented by the status quo are detailed in **Enclosure 3** of this Annex.

Annex A – Enclosure 1

List of Public Organizations

No.	Name of Public Organization
1	Airport Authority, Hong Kong
2	Architects Registration Board
3	Asbestos Administration Committee
4	Authorized Persons' and Registered Structural Engineers' Disciplinary Board Panel
5	Authorized Persons Registration Committee Panel
6	Board of Review (Inland Revenue Ordinance)
7	Broadcasting Authority
8	Chinese Medicine Council of Hong Kong
9	Chinese University of Hong Kong
10	Chiropractors Council
11	City University of Hong Kong
12	Clothing Industry Training Authority
13	Construction Industry Training Authority
14	Construction Workers Registration Authority
15	Consumer Council
16	Contractors Registration Committee Panel
17	Council of the Hong Kong Academy of Medicine
18	Council of the Hong Kong Institute of Certified Public Accountants
19	Council on Human Reproductive Technology
20	Dangerous Goods Standing Committee
21	Dental Council of Hong Kong
22	Disciplinary Board Panel (Land Survey)
23	Duty Lawyer Service
24	Education Commission
25	Electoral Affairs Commission
26	Employees Retraining Board
27	Engineers Registration Board
28	Equal Opportunities Commission
29	Estate Agents Authority
30	Fire Service (Installation Contractors) Disciplinary Board

No.	Name of Public Organization
31	Geotechnical Engineers Registration Committee Panel
32	Hong Kong Academy for Performing Arts, The
33	Hong Kong Applied Science and Technology Research Institute
34	Hong Kong Arts Centre
35	Hong Kong Arts Development Council
36	Hong Kong Baptist University
37	Hong Kong Council for Academic Accreditation
38	Hong Kong Council on Smoking and Health
39	Hong Kong Cyberport Management Company Limited
40	Hong Kong Deposit Protection Board
41	Hong Kong Examinations and Assessment Authority
42	Hong Kong Export Credit Insurance Corporation
43	Hong Kong Institute of Education
44	Hong Kong Internet Registration Corporation Limited (HKIRC)
45	Hong Kong Monetary Authority
46	Hong Kong Mortgage Corporation Limited
47	Hong Kong Polytechnic University
48	Hong Kong Productivity Council
49	Hong Kong Science and Technology Parks Corporation
50	Hong Kong Sports Institute Limited
51	Hong Kong Tourism Board
52	Hong Kong Trade Development Council
53	Hong Kong University of Science &Technology
54	Hospital Authority
55	Housing Managers Registration Board
56	Human Organ Transplant Board
57	Independent Commission Against Corruption
58	Independent Police Complaints Council
59	Kowloon-Canton Railway Corporation
60	Land Surveyors Registration Committee
61	Law Reform Commission of Hong Kong
62	Legal Aid Services Council
63	Legislative Council, The
64	Lingnan University
65	Liquor Licensing Board
66	Mandatory Provident Fund Schemes Authority

No.	Name of Public Organization
67	Medical Council of Hong Kong
68	Midwives Council of Hong Kong
69	MTR Corporation Ltd.
70	Nursing Council of Hong Kong
71	Occupational Safety and Health Council
72	Official Solicitor's Office
73	Ombudsman, Office of The
74	Open University of Hong Kong
75	Outward Bound Trust of Hong Kong Ltd., The
76	Pharmacy and Poisons Board
77	Planners Registration Board
78	Prince Philip Dental Hospital
79	Privacy Commissioner for Personal Data
80	Public Service Commission
81	Quality Education Fund
82	Radiation Board
83	Registered Contractors' Disciplinary Board Panel
84	Review Panel (Land(Miscellaneous Provision) Ordinance)
85	Securities and Futures Commission
86	Security and Guarding Services Industry Authority
87	Social Workers Registration Board
88	Sports Federation & Olympic Committee of Hong Kong, China
89	Standing Commission on Civil Service Salaries and Conditions of Service
90	Standing Committee on Directorate Salaries and Conditions of Service
91	Standing Committee on Disciplined Services Salaries and Conditions of Service
92	Standing Committee on Judicial Salaries and Conditions of Service
93	Structural Engineers Registration Committee Panel
94	Supplementary Medical Professions Council
95	Surveyors Registration Board
96	Town Planning Appeal Board
97	Town Planning Board
98	Transport Complaints Unit
99	Trust Funds, Temples and Cemeteries Joint Secretariat
100	University Grants Committee
101	University of Hong Kong

No.	Name of Public Organization
102	Urban Renewal Authority
103	Veterinary Surgeons Board
104	Vocational Training Council

Annex A – Enclosure 2

List of Regulatory Bodies/Sectors

No.	Name of Regulatory Body	Regulated Sector
1	Architects Registration Board	Registered architects on individual basis
2	Asbestos Administration Committee	Environmental sector
3	Authorized Persons' and Registered Structural Engineers' Disciplinary Board Panel	Professionals in the building and construction industry
4	Authorized Persons Registration Committee Panel	Professionals in the building and construction industry
5	Broadcasting Authority	Broadcasting sector
6	Chinese Medicine Council of Hong Kong	Chinese medicine practitioners
7	Chiropractors Council	Chiropractors
8	Construction Workers Registration Authority	Construction workers
9	Contractors Registration Committee Panel	Building and construction industry contractors
10	Council on Human Reproductive Technology	Hospital, institutions and clinics carrying out reproductive technology procedures and relevant activities under the scope of the Human Reproductive Technology Ordinance (Cap 561)
11	Dental Council of Hong Kong	Dentists
12	Department of Health	Medical and health
13	Disciplinary Board Panel (Factories and Industrial Undertakings (Safety Management) Regulation)	Industrial
14	Disciplinary Board Panel (Land Survey)	Land surveyors

No.	Name of Regulatory Body	Regulated Sector
15	Disciplinary Tribunal Panel (Builders' Lifts and Tower Working Platforms (Safety))	Contractors of builders' lift and tower working platform
16	Electrical and Mechanical Services Department	Electrical contractors
17	Electrical and Mechanical Services Department	Electricity - scheme of control (agreements)
18	Electrical and Mechanical Services Department	Electricity suppliers
19	Electrical and Mechanical Services Department	Gas supply companies
20	Electrical and Mechanical Services Department	Household electrical product suppliers
21	Electrical and Mechanical Services Department	Lift and escalator engineering
22	Estate Agents Authority	Estate agents
23	Fire Service (Installation Contractors) Disciplinary Board	Fire services installation contractors
24	Fire Services Department	Fire services installation contractors
25	Geotechnical Engineers Registration Committee Panel	Geotechnical engineers
26	Hong Kong Monetary Authority	Banking sector
27	Human Organ Transplant Board	Regulate related activities according to the Human Organ Transplant Ordinance (Cap. 465)
28	Land Surveyors Registration Committee	Land surveyors
29	Liquor Licensing Board	Premises licensed for the sale or supply of liquor for consumption on the premises
30	Mandatory Provident Fund Schemes Authority	Mandatory provident fund schemes providers
31	Medical Council of Hong Kong	Medical practitioners

No.	Name of Regulatory Body	Regulated Sector
32	Midwives Council of Hong Kong	Midwives
33	Nursing Council of Hong Kong	Nurses
34	Office of the Commissioner of Insurance	Insurance sector
35	Office of the Government Chief Information Officer - CARO	Recognized certification authorities
36	Office of the Telecommunications Authority	Telecommunications industry
37	Pharmacy and Poisons Board	Pharmacy and poisons professionals
38	Radiation Board	Radiation professionals
39	Registered Contractors' Disciplinary Board Panel	Building and construction industry contractors
40	Securities and Futures Commission	Exchanges and clearing houses
41	Securities and Futures Commission	Securities and futures sector
42	Securities and Futures Commission	Share registration
43	Security and Guarding Services Industry Authority	Private security and guarding services industry
44	Social Welfare Department	Child care sector providing day care service
45	Social Welfare Department	Voluntary residential drug treatment and rehabilitation sector
46	Social Welfare Department	Residential care homes for the elderly
47	Social Workers Registration Board	Individual registered social workers
48	Structural Engineers Registration Committee Panel	Structural engineers
49	Supplementary Medical Professions Council	Supplementary medical professions
50	Transport Department	Driving training
51	Transport Department	Transport sector - franchised bus companies

No.	Name of Regulatory Body	Regulated Sector
52	Transport Department	Transport sector - franchised bus (Long Win Bus Company)
53	Transport Department	Transport sector - franchised bus (New Lantao Bus Company (1973) Limited)
54	Transport Department	Transport sector - franchised bus (CityBus Limited)
55	Transport Department	Transport Sector – railway (Kowloon-Canton Railway Corporation)
56	Transport Department	Transport Sector - railway (MTR Corporation Limited)
57	Transport Department	Transport facilities management sector
58	Veterinary Surgeons Board	Veterinary sector

Exposures in Public Organizations Represented By Status Quo

Key Aspects	Exposures Represented By Status Quo
1. Security Management	
(a) Policy/Management Governance	Without the policy and management directives and guidance from the top, the organization can at best only rely on technical measures to protect its information asset. The most important human element remains to be a significant weakness that is most vulnerable to cyber attacks and data leakage.
(b) Operational Protection Measures	Insufficient operational protection measures will certainly expose the information asset of the organization to exploitation that may lead to their reliability and integrity at stake.
(c) Contingency Handling	In the absence of business contingency planning and rehearsals practiced by all staff, the organization cannot respond to and recover from any outbreak of information security incidents. There will be varying degrees of detrimental effects to customer services and business operation.
(d) Staff Awareness and Training	Staff awareness and training on information security is the only way to ensure the information security policy, measures and procedures are complied with. Failure to uphold this important aspect will lend the organization vulnerable to all kinds of cyber security threats.
(e) Security Risk Assessment and Audit	Security threats, loopholes and malpractices that are not addressed in a timely manner will increase the chance of cyber attacks as well as defeat the capability to continue business operation when hit by any security incidents.

Key Aspects	Exposures Represented By Status Quo
2. Security Governance	
(a) Test of Compliance	Security measures may become obsolete or unworkable over time due to business, application system, technology or other circumstantial changes unless regular review and compliance testing are performed to identify and verify the necessary improvements.
(b) Supportive and Random Checks	The occurrence of unanticipated or un-coordinated system exceptions or undetected non-compliances may develop into disastrous situations.
(c) Advice or Encouragement	Staff need to be updated, reminded and encouraged regularly on information security matters, otherwise they may overlook problems or not comply with the information security requirements leading to exposures to cyber security threats. This is especially important in catering for staff movement and changes.
3. Handling of Restricted/Classified Data	
(a) Operational Measures	The organization will be at risk in data integrity exposure or leakage unintentionally or due to malicious attacks.
(b) Technical Tools	Without the use of necessary technical tools, data integrity or confidentiality may be compromised during storage or transmission by unauthorized or unethical data access.
4. Arrangement in IT Outsourcing	
(a) Contractual Provisions	There will not be compliance obligations of the contractor with information security requirements and the matter will be left to the unknown practices of the contractor.
(b) Quality Assurance and Control	It will not be possible to assure the quality requirements to be implemented by the contractor and will lead to information security loopholes or problems.
(c) Security Governance and Control	The information system and data handled by the contractor cannot be assured without the necessary security control put in place.

Key Aspects	Exposures Represented By Status Quo
(d) Personnel Security Vetting	The organization may be at risk when unvetted personnel holding critical roles are assigned to handle highly sensitive data.
5. Technology Measures	
(a) Basic Measures	The organization will be prone to cyber attacks due to weaknesses in the defensive measures (e.g. virus, worms, intrusion, data leakage).
(b) Special Data Handling Measures	Such data will be vulnerable to attack during transmission, storage and disposal.
(c) More Advanced Authentication/ Access Control Technologies	Transactions demanding higher security protection will not be safe without proper authentication to ensure the confidentiality, integrity and non-repudiation requirements are met.
(d) Network Related	The data transported across the unsecured networks cannot be guaranteed on its integrity and confidentiality.
(e) Asset Protection	Without physical security protection, any other security measures put in place are not meaningful and cannot be made effective.
6. Staff Awareness, Education and Training	
(a) Facilitation	Unless the staff are educated and trained on information security, they may violate or undo the information security policy and guidelines making the organization more vulnerable to cyber attacks.
(b) Incentive for Staff to Acquire Information Security Qualification	Staff may lack the interest or are slow to learn or acquire the necessary skills in implementing or enforcing effective information security programmes for the organization.
(c) Periodic Reminder	Staff may misunderstand, forget or violate the information security requirements especially when there are staff movement and changes.

Annex B

Information Security Promotion and Education Programme

Channels	**Activities Description**	**Dates**
Resources on Website	● A theme page to promote the "Hong Kong Clean PC Day 2006" Campaign was set up on the one-stop Information Security website (www.infosec.gov.hk) ● Publish reference information on international information security standards and professional certifications on the website	September 2006 December 2006
Seminars	● Collaborate with HKPF and HKCERT in organizing information security seminars free-of-charge for the general public ● Collaborate with HKCERT and professional associations in organizing public conference to promulgate international information security standards and professional certifications	November 2006 March 2007
Radio Programmes	● A series of radio programmes being broadcast focusing on how to protect data privacy and proper use of security protection software on PC	July 2006 – March 2007
TV Episodes	● A series of "Police Report" broadcast focusing on protection of wireless network, mobile devices and data privacy	November 2006

Channels	**Activities Description**	**Dates**
Publications	● Publicity leaflets emphasizing on the importance and measures to keep PC clean distributed to the public through various channels e.g. libraries, community halls, schools, uniformed organizations, etc.	October 2006
Carnival	● A "Hong Kong Clean PC Day 2006" Carnival held	25 November 2006