For Discussion **Paper No. 9/2011**
on 3 November 2011

DIGITAL 21 STRATEGY ADVISORY COMMITTEE

Cyber Security

Purpose

This paper briefs Members on the global cyber security outlook facing governments of some countries and their strategy and efforts in addressing cyber security challenges. It also briefs Members on the cyber security posture in Hong Kong as compared to these countries.

Background

2. Like other countries and economies, the Government, businesses and citizens in Hong Kong rely heavily on information and communications technology (ICT) and the Internet in their business operations and daily lives. At the same time, cyber criminals or malicious attackers are also employing advanced technologies to carry out illegal or illicit activities. The cyber space, which comprises the telecommunications infrastructure, critical information infrastructure and systems, becomes a domain that should be better protected for public security and economic prosperity.

Global Cyber Security Outlook

3. Cyber crime, or computer crime, in general refers to any crime in the cyber space that involves a computer and a network. Various statistics on cyber crime show a rising trend. For example, the number of measured web-based attacks in the world increased by

93% in 2010 compared to 2009[1]. The number of malicious websites increased by 111.4% from 2009 to 2010[2]. According to the Hong Kong Police Force (HKPF), 391 online business fraud cases were reported in the first half of 2011, representing an increase of 33% as compared with the same period the year before.

4. Cyber attack refers to a form of cyber crime using special software to cause the malfunctioning of targeted computer systems or networks resulting in information leakage, identity theft and/or disrupted businesses or services. A notable example was a series of cyber attacks targeting Estonia in 2007 which swamped websites of Estonian organisations, including the Estonian parliament, banks, ministries, newspapers and broadcasters. As a result, the public services in Estonia were affected for a few weeks.

Cyber Security Strategy

5. A number of countries or economies have formulated their cyber security strategy and are taking positive actions to respond to the cyber security threats. While different countries/economies are having different strategies and adopting different measures in tacking cyber security challenges, there are six common aspects that they have been pursuing. These include ***National Cyber Security Organisational Framework, Critical Infrastructure Protection, Legislation on Cyber Crime, Computer Emergency Response Team, Awareness Promotion for the Public*** and ***Capability Development***. In the **Annex,** we have made a brief comparison of Hong Kong among several countries including Australia, Japan, the U.K. and the U.S. with reference to each of these individual aspects.

[1] investor.symantec.com/ko/kr/phoenix.zhtml?c=89422&p=irol-newsArticle&ID=1546585

[2] http://www.websense.com/content/threat-report-2010-web-security.aspx

Cyber Security Posture of Hong Kong and Countries under Study

(a) <u>National Cyber Security Organisational Framework</u>

6. Some countries, such as the U.S. and the U.K., have established a special government agency or office with direct roles and responsibilities on cyber security. In the U.S., the Department of Homeland Security (DHS) plays an important role in countering cyber security threats. In the U.K., the Office of Cyber Security & Information Assurance (OCSIA) provides strategic direction and coordinates action relating to enhancing cyber security and information assurance.

7. The cyber security organisational framework and strategy in a country are developed according to their specific environment, culture and individual requirements. In some cases, the cyber security organisational framework and strategy are pitched at the national security level, with strong military and defense emphasis. For example, the U.S. Government has placed cyber security threats on equal footing with military and economic threats. Under Japan's "National Defense Program Guidelines for FY 2011 and beyond", the country will strengthen its posture and response capability to deal with cyber attacks.

8. In Hong Kong, the national and military angles are clearly not applicable. The Security Bureau (SB) and the Office of the Government Chief Information Officer (OGCIO) provide guidance and advice to bureaux and departments (B/Ds) on information security. SB and OGCIO work closely to keep surveillance on any emerging cyber security threats, examine and tackle cyber security issues and continue to introduce additional measures to strengthen our cyber security posture.

(b) <u>Critical Infrastructure Protection</u>

9. The definition of critical infrastructure varies amongst the economies studied. In general, it refers to those infrastructures

which when incapacitated or destructed would have a debilitating impact on the economy's security and socio-economic well-being. All the economies under study recognise the importance of public-private partnerships in critical infrastructure protection. Such partnerships may be government-led, private sector-led, or joint initiatives. A major challenge is to strike a proper balance between security requirements and business efficiency imperatives. While governments often put emphasis on the risks brought about by cyber crimes, the private sector running the infrastructure may consider measures to mitigate such risks as a financial burden in operating costs.

10. In Hong Kong, the critical infrastructures are either owned by the Government or under the governance of respective regulatory mechanisms. Since regulatory bodies are the domain experts of their respective regulated sectors, it would be most effective and appropriate for them to determine the extent of the regulatory measures including those in relation to information security and cyber threats. On the protection of the local Internet infrastructure, the OGCIO set up the Internet Infrastructure Liaison Group[3] (IILG) in 2005 to provide a platform for communication and exchanges on issues concerning the stability, security, availability and resilience of the local Internet infrastructure. The IILG collaborates among the relevant stakeholders during major events or situations with emerging information security threats. The HKPF and the OGCIO stand ready to render advice and assistance to B/Ds as and when necessary on information security enhancement measures for regulated bodies/sectors under their purview.

(c) <u>Legislation on Cyber Crime</u>

11. In the economies studied, it is often the case that cyber crimes are considered adequately dealt with under existing legislation albeit with some necessary modifications in their language and terms, particularly relating to their scope of application

[3] The IILG comprises members from Hong Kong Internet Exchange, Hong Kong Internet Registration Corp. Ltd., Hong Kong Internet Service Providers Association, Hong Kong Computer Emergency Response Team Coordination Centre, Office of the Telecommunications Authority, HKPF and OGCIO.

as determined by their definition and interpretation. For example, in the U.S., the Homeland Security Act 2002 was enacted with a purpose related to cyber security. It also led to the establishment of the DHS and other security provisions.

12. Hong Kong does not have a targeted piece of legislation to counter cyber crimes. Most of the existing legislation is technology neutral and can apply equally to activities in a cyber environment. Relevant ordinances are reviewed and amended as necessary from time to time to take account of the changing environment.

(d) Computer Emergency Response Team

13. The economies under study have established Computer Emergency Response Team (CERT) services such as warnings, alerts and assistance in resolving security incidents to the public sector. CERT usually plays an active role in drill exercises that simulate cyber security events and attacks. For example, the United States-Computer Emergency Readiness Team (US-CERT) participates in the Cyber Storm drill hosted by the DHS. The Asia Pacific Computer Emergency Response Team (APCERT) has been conducting annual drills since 2004 to test the timeliness and response capability of its members.

14. The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), operated by the Hong Kong Productivity Council (HKPC), plays a key role in the protection of the local cyber environment. One of the core functions of HKCERT is to serve as a focal point in Hong Kong for computer security incident reporting and response. HKCERT also provides assistance to the community in the protection against computer security threats, in the prevention of hacking attacks and in recovery actions for computer security incidents. The OGCIO and HKPC jointly review and enhance the service of HKCERT according to cyber security trends and public needs from time to time.

15. The HKCERT has also organised local information security

incident response drills annually since 2009, to ascertain the responsiveness by local key Internet stakeholders against cyber attacks. Through the exercise the participants can gain experience on how to respond to emergency conditions and the organiser can gain insights on how to coordinate and improve communication amongst the stakeholders during major incidents. HKCERT also participated in some of the APCERT drill exercises[4].

(e) *Awareness Promotion for the Public*

16. Just as governments must be aware of the potential for a cyber attack to occur, businesses and individuals must also take steps to protect their computer and information assets from cyber attacks. All of the economies under study have set up public websites providing information security related information for reference by the community. They also have established annual awareness promotion programmes for the public.

17. In Hong Kong, the OGCIO has set up the INFOSEC website (www.infosec.gov.hk) in 2002 to provide a one-stop portal facilitating the public to access various information security related resources and updates. To raise public awareness on information security and strengthen the protection of their computer and information assets from cyber attacks, the OGCIO, HKPF and HKCERT have jointly organised an annual promotion campaign "Hong Kong Clean PC Day"[5] since 2005. The theme of the 2011 campaign is "Mobile Security" with a variety of activities including public seminars, stakeholders symposium, contests, and school visits which are being conducted throughout the year.

(f) *Capability Development*

18. There are various security certifications that organisations can seek to demonstrate their compliance to internationally

[4] The APCERT drill 2011, with the theme "Critical Infrastructure Protection", was held in February 2011 and participated by 15 economies including Australia, India, Japan, Korea, the Mainland of China, Malaysia, Singapore and Hong Kong.

[5] The campaign in the brand name of "Hong Kong Clean PC Day" will be renamed tentatively to "Build a Secure Cyber Space" starting from 2012 in light of the evolving nature of security threats.

recognised security standards. For example, ISO-27001 of the International Organisation for Standardisation (ISO) is the formal international standard against which organisations may seek independent certification of their information security management systems. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System, using a continual improvement approach. Many countries around the world have adopted ISO-27001 as their framework for devising information security measures. Japan, being the most aggressive, has used ISO-27001 as a basic requirement for public contracts with IT systems. For individuals, there are professional security certifications, such as Certified Information Systems Security Professional (CISSP) of International Information Systems Security Certification Consortium, Inc. and Certified Information Systems Auditor (CISA) of Information Systems Audit and Control Association.

19. In Hong Kong, there are 32 organisations certified with ISO-27001[6] as at September 2011. For individuals, the Continuing Education Fund administered by the Student Financial Assistance Agency provides subsidy for relevant courses leading to certification (including CISSP and CISA). There are a number of local organisations or global organisations with Hong Kong chapters formed to promote technical, security and ethical standards in the IT industry. They organise various security seminars and conferences throughout the year for boosting local capability. In the Government, we promote the adoption of high security standards and take the lead to require IT outsourcing contractor staff to possess relevant security certifications and qualifications. We also give strong support to our staff (e.g. examination fees refund) in seeking these security certifications and qualifications. We will continue to encourage business organisations and IT professionals to acquire security certifications and qualifications and support organising local security events so as to develop our overall capability in addressing cyber security threats.

[6] www.iso27001certificates.com/Register%20search.htm. Government departments include HKPF and Customs and Excise Department have some organisational functions obtained the certification.

Conclusion

20. Cyber crime and attacks are threats to our public security and economic prosperity. We will continue to keep surveillance on any emerging cyber security threats and consider additional measures to strengthen our cyber security posture.

Advice Sought

21. Members are invited to note the contents of this paper and provide their comments.

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau
November 2011

Annex

Comparison of Cyber Security Aspects among Different Economies

Cyber Security Aspects	Australia	Japan	U.K.	U.S.	Hong Kong
1. National cyber security organisational framework	The Attorney-General's Department is the lead agency for cyber security policy across the Australian Government. It chairs the Cyber Security Policy and Coordination Committee, which is the interdepartmental committee that coordinates the development of cyber security policy for the Australian Government.	The Information Security Policy Council (ISPC), established under the Cabinet Secretariat in 2005, sets basic strategies for information security policy. The ISPC comprises the National Public Safety Commission chairman, the defense minister and private-sector experts.	The Office of Cyber Security and Information Assurance (OCSIA) was established in the Cabinet Office in 2009. The OCSIA has overall ownership of the cyber security strategy and provides strategic leadership across government for cyber security issues.	The Department of Homeland Security (DHS) has the leading role in critical infrastructure protection and cyber security. In 2009, the U.S. President appointed a cyber security coordinator to coordinate cyber security policy across the federal government, from the military to civilian agencies.	National organisational framework is not applicable. Security Bureau (SB) and Office of the Government Chief Information Officer (OGCIO) provides guidance and advice to bureaux and departments (B/Ds) on information security.

Cyber Security Aspects	**Australia**	**Japan**	**U.K.**	**U.S.**	**Hong Kong**
2. Critical infrastructure protection (CIP)	The CIP Program was created in 2003. Its primary focus is to share information and best practice with the owners and operators of critical infrastructure, strengthen and improve their security measures and help achieve better risk management.	Action Plan on Information Security Measures for Critical Infrastructures was published by the ISPC in 2005 and revised in 2009. The Plan includes definitions of critical infrastructure elements and threats, safety standards for information security, information-sharing systems in public-private partnerships (PPP), interdependency analyses, and development of various mechanisms.	The Centre for the Protection of National Infrastructure (CPNI), set up in 2007, is the agency charged with providing advice to any entity within the U.K. that owns or operates services or property critical to commerce, public health or security.	Homeland Security Presidential Directive 7, which was issued in December 2003, identified 17 critical infrastructures and key resources. The National Infrastructure Protection Plan (NIPP) issued by the DHS in June 2006 provides an overall framework for existing and future programs and activities for the protection of critical infrastructures and key resources.	On the protection of the Internet infrastructure, the Internet Infrastructure Liaison Group (IILG) was set up in 2005 to provide a platform for communication and exchanges on issues concerning the stability, security, availability and resilience of the local Internet infrastructure.

Cyber Security Aspects	**Australia**	**Japan**	**U.K.**	**U.S.**	**Hong Kong**
3. Legislation on cyber crime	The Cybercrime Act 2001 - An Act to amend the law relating to computer offences, and for other purposes. In June 2011, the Australian Government introduced cyber crime legislation to the Parliament to combat global cyber attacks.	The Unauthorised Computer Access Law No. 128 of 1999 prohibits acts of unauthorised computer access (Article 3) as well as acts that facilitate unauthorised computer access (Article 4).	The main cyber crime law is the Computer Misuse Act, which includes offences of unauthorised access to computer material and of unauthorised modification of computer material. The Act was amended in 2008.	The Homeland Security Act of 2002 is the foundation for many other initiatives including the setting up of the Department of Homeland Security, the Critical Infrastructure Information Act of 2002, and the Cyber Security Enhancement Act of 2002.	Hong Kong does not have a targeted piece of legislation to counter cyber crimes.

Cyber Security Aspects	**Australia**	**Japan**	**U.K.**	**U.S.**	**Hong Kong**
4. Computer Emergency Response Team (CERT)	CERT Australia is the national coordination point for the provision of cyber security information and advice for the Australian community. CERT Australia provides their citizens with access to information on cyber threats and vulnerabilities, and information on how to better protect themselves. CERT Australia has participated in the APCERT (CERTs in Asia Pacific) drill.	JPCERT/CC was established in 1992. The center has been gathering information on computer incidents and vulnerabilities, issuing security alerts and advisories, and providing incident responses as well as education and training to raise awareness of security issues. JPCERT/CC has participated in the APCERT drill.	The GovCertUK provides warnings, alerts and assistance in resolving serious IT incidents for the public.	US-CERT is responsible for analysing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. US-CERT has participated in the Cyber Storm drill hosted by the DHS.	HKCERT serves as a focal point for computer security incident reporting and response. It provides assistance to the community in the protection against computer security threats, in the prevention of hacking attacks and in recovery actions for computer security incidents. HKCERT participated in some of the APCERT drill exercises.

Cyber Security Aspects	**Australia**	**Japan**	**U.K.**	**U.S.**	**Hong Kong**
5. Awareness promotion for the public	"National Cyber Security Awareness Week" is held each year in partnership with industry and community organisations. It aims to educate home and small business users on the simple steps they can take to protect their personal and financial information online. "www.staysmartonline.gov.au" is a website for cyber security information for Australian home users and small businesses.	"Information Security Month" campaign has been held since 2010. Events on information security, such as seminars, were held nationwide by related government agencies and corporations. "www.npa.go.jp/cyberpolice/english" is an Internet Security Portal Site which provides information gathered by the police on information security to Internet users, and aims at increasing security awareness.	"Get Safe Online Week" will be held in the 2nd week in November 2011. The Cabinet Office supports raising awareness of cyber security through a partnership programme with the private sector as well as law enforcement agencies. Get Safe Online website "www.getsafeonline.org" provides security information for citizens and businesses.	Since 2004, October has been designated "National Cyber Security Awareness Month". DHS hosted a website "www.dhs.gov/files/cybersecurity.shtm" where citizens can access cyber security tips, identify Internet hoaxes, protect themselves online, and learn how privacy protections are integrated into cyber security activities.	OGCIO, HKPF and HKCERT jointly collaborate with the IT industry to promote security awareness to the public. Since 2005, the "Hong Kong Clean PC Day" campaign is arranged annually with a particular theme. The one-stop portal "www.infosec.gov.hk" provides latest news and up-to-date reference on information security matters for reference by the public.

Cyber Security Aspects	**Australia**	**Japan**	**U.K.**	**U.S.**	**Hong Kong**
6. Capability development	Australia has obtained 29 ISO-27001 certifications.	Japan has 3,862 ISO-27001 certificates (out of a worldwide total of 7,346). This is due to the fact that the Japanese Ministry of Economy, Trade and Industry (METI) mandates that companies that do business with the Japanese government need to be ISO-27001 certified.	477 U.K. companies have achieved ISO-27001 certification so far.	ISO-27001 certification in the U.S. is gradually increasing due to commercial desire to meet the expectations of stakeholders. The number increased from 69 in 2006 to 101 at present.	There are 32 organisations certified with ISO-27001. For individuals, subsidy is provided for relevant courses leading to certification (including Certified Information Systems Security Professional and Certified Information Systems Auditor) under the Continuing Education Fund.