Report on the Institutional Review of Computer Emergency Response Centre Services in Hong Kong

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau
The Government of the Hong Kong Special Administrative Region

October 2008

Table of Contents

Foreword

The Government Chief Information Officer (GCIO) has recently completed an institutional review of the Computer Emergency Response Centre (CERC) services in Hong Kong. This Report documents the findings and recommendations, and invites views from the industry regarding the mechanisms for giving input into the priorities, goals and service levels of CERC services in Hong Kong.

Comments may be forwarded to the Government Chief Information Officer on or before **14 November 2008** by any of the following means:

Post:	Government Chief Information Officer Office of the Government Chief Information Officer 6/F, Cyberport 1 100 Cybeport Road Hong Kong **(Attn.: Systems Manager (E)21A)**
Fax:	(852) 2989 6073
Email:	cerc_review@ogcio.gov.hk

We assume that all submissions are not made in confidence unless specified otherwise. We may reproduce and publish the submissions in whole or in part in any form and use, adapt or develop any proposals put forward without seeking permission from or providing acknowledgement to the party making the proposal.

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau
October 2008

Background

The tremendous growth in the use of information technology and the Internet for e-Commerce has been accompanied by exponential growth of computer security intrusion in recent years. Information security has become an important issue in sustaining the vision of the Digital 21 Strategy to develop Hong Kong as a leading digital city in a globally connected world. It is generally considered that awareness, vigilance and prevention are critical measures to safeguard against and minimize the impact of security incidents.

2. Back in December 1988, the CERT Coordination Center (CERT/CC)[1], operated by the Carnegie Mellon University for the US Department of Defense, was established after a computer security incident which brought about 10 percent of the Internet systems to a halt. Since then, the CERT/CC has gradually expanded its role to giving warning and alerts to the public about security threats and incidents with a view to containing the damage arising from such incidents.

3. In response to concerns over security threats to computer systems and the Internet, many economies and some large organizations have set up computer emergency response centres (CERCs) to serve as focal points for computer security incident reporting and for responding to local enterprises and Internet users in network security incidents. Typically, a CERC coordinates responses and recovery actions, disseminates security-related information, identifies vulnerabilities and takes preventive measures against security threats. It also organizes awareness programmes, training courses, and conferences on information security and maintains close liaison with its local and overseas counterparts.

4. There are now around 200 CERC related organizations serving various users and sectors in more than 40 economies worldwide that deal with cyber security response and related services. In this Report, we

[1] Further information on CERT/CC can be found in the website http://www.cert.org.

refer to such services collectively as CERC services.

5. Generally, there are two types of CERC related organizations worldwide. One type mainly serves commercial, academic or government organizations, and focuses on and provides services and support to its defined constituency, whereas the other type serves the whole community across a broad spectrum of sectors within an economy. In this exercise, we focus on the institutional review on services provided by the latter type of CERC in Hong Kong.

Impact of Information Security Incidents

6. In recent years, the fast adoption of the Internet channel has fuelled the rapid development of e-Commerce in the global business environment. Since 2001, the value of business transactions from selling of goods, services or information through electronic means in Hong Kong amounted to over $195 billion. It is observed that over the years the number of computer security incidents reported in Hong Kong has been increased by more than seven-fold between 2001 and 2007 of which phishing incidents has increased by more than ten-fold during 2004 and 2007. The financial loss due to computer crime cases in Hong Kong amounted to over $50 million since 2001.

7. With reference to overseas experience, even a single cyber attack incident can cause huge impact on a national scale. In April 2007, the Baltic nation of Estonia experienced a very serious Internet attack on Government ministries, banks, newspaper and political parties throughout the country. Around one million computers located in more than 50 countries worldwide were involved in the attack which had crippled the normal operations of the country for many days. In December 2006, TJX, a public company in the US reported that their computer systems had been intruded and information of more than 45 million credit cards was stolen. As a result, TJX was expected to face a total expense of nearly US$1 billion in settlement of the consequence of the incident.

8. In view of the potentially high financial loss from computer crimes and large transaction value associated with electronic business, a reliable and secure cyber environment is essential for the conduct of electronic business transactions over the Internet.

CERC Services of Hong Kong

9. In 2001, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)[2] was established under the Hong Kong Productivity Council (HKPC) to provide a centralized contact on computer and network security incident reporting and response for local enterprises especially small-to-medium sized enterprises (SMEs), and Internet users in case of security incidents. It also coordinates response and recovery actions for reported incidents, helps monitor and disseminate information on security related issues, advises on preventive measures against security threats, as well as organizes awareness seminars and training courses on information security related topics.

Institutional Review of the CERC Services

10. The CERC for Hong Kong plays an important role in facilitating Hong Kong to have a reliable and secure environment for doing business. With regard to the rapidly changing Internet environment, the Government Chief Information Officer (GCIO) has reviewed the CERC services for Hong Kong with a view to setting our direction and establishing a long-term and sustainable arrangement for the CERC services.

11. The review has examined the most appropriate long-term arrangement of the CERC services for Hong Kong, while taking the latest international and regional developments into consideration. References

[2] Further information on the HKCERT can be found in its website at http://www.hkcert.org.

have been made to the practices of eight other economies (viz. Australia, Canada, the Mainland of China, India, Japan, Malaysia, Singapore, and the United States). A comparison of the current CERC services for Hong Kong and these economies is highlighted in **Appendix I**.

Need for a CERC for Hong Kong

12. It is observed that many digitally leading economies have generally established their CERCs. In view of the significant adverse impacts of information security incidents (paragraphs 6 to 8), the provision and quality of CERC services to our local enterprises and Internet users is essential to our maintenance of a reliable and secure Internet environment by helping computer users to minimize services disruption, reduce loss and facilitate business operation recovery after information security incidents.

Institutional Arrangement for Setting up the CERC

13. In most of the overseas economies, the CERCs are set up and operated by non-profit making and neutral bodies or their governments. This common practice will be adopted in Hong Kong and to implement this, the HKPC, a non-profit making body in Hong Kong will continue to operate the HKCERT to provide the CERC services for the community.

Funding Arrangement

14. In order to maintain the stability and neutrality in the provision of CERC services, the Government will provide funding to support HKCERT's operation. The funding is meant to cover the essential services only. However, the HKCERT will be allowed to offer other chargeable value added services if considered appropriate by the Government on a case-by-case basis.

CERC Services Scope

15. In order to sustain a reliable and secure cyber environment for doing business in Hong Kong, the following types of CERC services are essential in order to help the local enterprises and Internet users prevent and minimize service disruption and avoid attacks on the Internet:

- Incident handling, response and coordination
- Dissemination of alerts, warnings and security-related information
- Security awareness building and training
- Coordination and collaboration with relevant parties on security preventive measures

Seeking of Industry’s Views

16. The HKPC has proposed to Government the operation of the HKCERT in 2009/10 as well as some future plans beyond 2009/10. Details of HKPC’s proposal are attached in **Appendix II**.

17. On the aspects of governance and performance monitoring, HKPC proposed that besides the senior management of HKPC oversees the functions and operations of HKCERT and directs the strategy of the centre, the following new mechanisms will be introduced –

(a) HKCERT will prepare an annual report on the achievement of the centre each year. The report will be submitted to OGCIO and presented to the HKPC industry cluster, as well as posted on the HKCERT website for public reference.

(b) The management of the HKCERT will meet with OGCIO twice a year, to discuss the operations and activities performed, and agree on the upcoming strategies and programmes of the centre. The meeting could also be used as a forum to evaluate the performance of HKCERT.

18. We welcome views of the industry on the governance and performance monitoring mechanism of HKCERT. In particular, the industry may suggest mechanisms for giving input into the priorities, goals, service levels of CERC services and so forth. We will take the suggestions into consideration in the implementation of the new CERC regime.

Appendix I – Highlights of CERC Services for Hong Kong and Other Economies

	Hong Kong HKCERT	**Australia AusCERT**	**Canada CCIRC**	**Mainland of China CNCERT/CC**	**India CERT-In**	**Japan JPCERT/CC**	**Malaysia MyCERT**	**Singapore SingCERT**	**United States US-CERT**
Established in	2001	1993	2005	2000	2004	1996	1997	1997	2003
CERC Services - Incident Handling, Response and Coordination									
• Provide 24x7 incident reporting and responding service	✓	✓	✓	✓	✓	✓	✓	✓	✓
• Coordinate with various parties including other CERCs	✓	✓	✓	✓	✓	✓	✓	✓	✓
• Multiple reporting channels (e.g. email, fax, telephone, SMS, etc.)	✓	✓	✓	✓	✓	✓	✓	✓	✓

	Hong Kong HKCERT	**Australia AusCERT**	**Canada CCIRC**	**Mainland of China CNCERT/CC**	**India CERT-In**	**Japan JPCERT/CC**	**Malaysia MyCERT**	**Singapore SingCERT**	**United States US-CERT**
CERC Services - Dissemination of Alerts, Warnings and Security-related Information									
• Disseminate security related information (e.g. security alerts, warnings, and vulnerabilities)	✓	✓	✓	✓	✓	✓	✓	✓	✓
• Publish guidelines, reports, newsletters, survey, etc.	✓	✓	✓	✓	✓	✓	✓	✓	✓
• Multiple dissemination channels (e.g. website, SMS, RSS, mailing lists, etc)	✓	✓	✓	✓	✓	✓	✓	✓	✓

	Hong Kong HKCERT	**Australia AusCERT**	**Canada CCIRC**	**Mainland of China CNCERT/CC**	**India CERT-In**	**Japan JPCERT/CC**	**Malaysia MyCERT**	**Singapore SingCERT**	**United States US-CERT**
CERC Services - Security Awareness Building and Training									
• Provide seminars, workshops and training courses on computer security related issues	✓	✓	✓	✓	✓	✓	✓	✓	✓
CERC Services – Coordination and Collaboration with Relevant Parties on Security Preventive Measures									
• Collaborate with various parties (e.g. Internet stakeholders, law enforcement agencies, vendors, etc.)	✓	✓	✓	✓	✓	✓	✓	✓	✓
• Monitor cyber threat / Internet health	Limited services	✓	✓	✓	Information not available	✓	Information not available	✓	✓

	Hong Kong HKCERT	**Australia AusCERT**	**Canada CCIRC**	**Mainland of China CNCERT/CC**	**India CERT-In**	**Japan JPCERT/CC**	**Malaysia MyCERT**	**Singapore SingCERT**	**United States US-CERT**
• Provide free security scanning service	No	Information not available	Information not available	Information not available	Information not available	Information not available	✓	Information not available	Information not available
• Participate regional and international CERT team initiatives	✓	✓	✓	✓	✓	✓	✓	✓	✓
• Conduct research and analysis on security related topics	Limited services	✓	Information not available	✓	✓	✓	✓	✓	✓
Institutional Arrangement for the Setting Up									
• By Government	-	-	✓	✓	✓	-	✓	✓	-
• By non-profit making body	✓	✓	-	-	-	✓ (with legal status)	-	-	-
• By public-private partnership	-	-	-	-	-	-	-	-	✓

	Hong Kong **HKCERT**	**Australia** **AusCERT**	**Canada** **CCIRC**	**Mainland of China** **CNCERT/CC**	**India** **CERT-In**	**Japan** **JPCERT/CC**	**Malaysia** **MyCERT**	**Singapore** **SingCERT**	**United States** **US-CERT**
Funding Arrangement									
• Funded by Government	✓	-	✓	✓	✓	✓	✓	✓	✓
• Self-financed	-	✓	-	-	-	-	-	-	-
Reference URL for Further Details									
	http://www.hkcert.org/english/home.html	http://www.auscert.org.au/index.html	http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx	http://www.cert.org.cn/index.shtml	http://www.cert-in.org.in/	http://www.jpcert.or.jp/english/	http://www.mycert.org.my/	http://www.singcert.org.sg/	http://www.us-cert.gov/

Note: The above highlights are information up to September 2008.

Appendix II –

Proposal from Hong Kong Productivity Council for the provision of Computer Emergency Response Centre Services in Hong Kong

Hong Kong
Productivity Council
香港生產力促進局

Service Proposal for
Hong Kong Computer Emergency Response Team
Coordination Centre (2009/10)

Prepared By

Hong Kong Productivity Council

October 2008

Table of Content

1. Purpose

The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) was established in 2001 with funding from the Innovation and Technology Fund (ITF) of the HKSAR Government. The centre was operated by the Hong Kong Productivity Council (HKPC) since then. The constituency of the centre includes local enterprises, in particular, small to medium sized enterprises, and Internet users.

The objectives of HKCERT are:

a) To serve as a centralized point in Hong Kong for computer security incident reporting and response;

b) To raise the awareness of computer security issues and to promote international standards and practices;

c) To help improve the security of systems and prevent computer security related incidents;

d) To assist and coordinate recovery actions for computer security incidents;

e) To maintain network with other Computer Emergency Response Team (CERT) organizations and Forum of Incident Response and Security Team (FIRST) to facilitate cooperation and coordination.

2. Background

HKCERT is a critical information infrastructure for Hong Kong. Locally, it is chartered to provide a centralized contact on computer incident reporting and responses to local enterprises and Internet users in case of network security incidents. Internationally, it is regarded as the “National Computer Security Incident Response Team” for Hong Kong, coordinating and collaborating with other CERT teams to solve issues relating to information security and computer incidents. Throughout the years, HKCERT had built up its technical expertise, community acceptance and trust on providing security alert, incident handling and security awareness services in Hong Kong.

Since its establishment, HKCERT has handled major incidents in Hong Kong, including:

a) The outbreaks of the SQL Slammer, Blaster worm and the Sasser worm in 2003 and 2004;
b) The massive spyware attack to the customers of local banks in 2005;
c) The Internet Health monitoring and reporting during the Sixth Ministerial Conference (MC6) of World Trade Organization (WTO) in 2005, the International Telecommunication Union (ITU) Telecom World Conference in 2006, and the Beijing Olympics and the Paralympic Games in 2008;
d) The assistance to the Hong Kong Domain Name Registration (HKDNR) in identifying and shutting down malicious websites registered under the .hk domain in 2008;
e) The proactive discovery of local websites defaced or infected by malicious codes in 2008.

Other than responding to incidents, HKCERT also helped in the prevention of computer viruses and security incidents by organizing public seminars and events to promote the public awareness, and published handbooks and guidelines on information security issues, including:

a) SME Information Security Guideline
b) Guideline for Prevention of Spyware and other Potentially Unwanted Software
c) Home PC Baseline Security Self-Assessment Checklist
d) "MarketScore" Removal Procedure
e) Handling Email Storm generated from Worms with Spoofed Sender
f) Guideline for Securing Wireless LAN Deployment
g) Guideline for Computer Virus Prevention
h) Guideline for Pretty Good Privacy

HKCERT also participated in a number of government working groups and committees, including the Internet Infrastructure Liaison Group (IILG), the Information Security Task Force, and the Wi-Fi Security Working group. HKCERT also represented Hong Kong in international CERT team coordination and meetings since 2001.

With the increase in e-commerce activities in Hong Kong, the functions of HKCERT have become an integral part of the Internet infrastructure in Hong Kong to build a safer environment on the Internet.

3. HKCERT Services and Operations in 2009/10

The scope of services for 2009/10 will be similar to those services provided currently. The areas of work will include:

a) Incident Report and Response

- Local incident report (problem identification and resolution)
    - To provide computer incident reporting 24 hours a day 7 days a week on incidents relating to malware infection, hacking and intrusion, and phishing email and websites
    - To accept incidents through telephone, fax and e-mail
    - To assist and coordinate recovery actions for computer incidents
    - To coordinate with various parties during the major outbreaks of security and virus incidents
- Overseas incident report (local and overseas coordination)
    - To coordinate the response to overseas incident reports
    - To communicate with local and overseas organizations to resolve the issue
- Proactive discovery of local defacement, hacked web site
    - To collect vulnerability and malicious website information
    - To search on .hk websites on possible infections
    - To inform owners of websites and advise on rectification
    - To follow-up with the owners on rectification status

b) Security Alerts and Early Warning

- Daily information gathering from the Internet
    - To closely monitor information on security related issues, such as the latest viruses, security weaknesses and countermeasures
- Alerts dissemination

    - To disseminate security information to the public via the HKCERT website, email, SMS and through mass media

c) Publications

- Monthly Newsletter
    - To publish a monthly newsletter providing latest information on computer and network security
- Alert Summary
    - To publish alert summary twice every month on security related alerts and news
- Guidelines and Checklists
    - To publish security-related guidelines and checklists on information security threats and countermeasures
- Security Articles and Advisories
    - To publish security related articles and advisories about security threats, vulnerabilities, defense strategies and early warning of likely attacks

d) Education, Training and Public Relations

- Clean PC Day Activities
    - To work with the Office of Government Chief Information Officer (OGCIO) and Hong Kong Police Force to organize activities in November / December to promote public awareness
- Speaking in public seminars
    - To speak in events to promote public awareness
- Press and Media
    - To communicate with press and media on information security issues and incidents.

e) Coordination and Collaboration

- Local committees and working groups

  - To meet and discuss with OGCIO and the Technology Crime Division of the Hong Kong Police Force regularly on issues of common interests and strategic plans for Hong Kong
  - To participate and support the working groups and committees organized by the HKSAR government, such as OGCIO and OFTA on information security issues
- ISPs and HKDNR
  - To work with HKDNR and ISPs (mainly through HKISPA) to resolve information security issues
- Information Security Vendors
  - To coordinate with information security and software vendors on information security incidents
- Overseas CERT teams
  - To coordinate with regional and international CERT teams to resolve information security issues and incidents
  - To participate in regional and international CERT team initiatives in information sharing and collaboration

4. Resources and Expenses

This part is left blank intentionally

5. Governance and Performance Monitoring

5.1 Governance

Currently, the senior management of HKPC oversees the functions and operations of HKCERT and directs the strategy of the centre. Since the services provided by HKCERT is unique and that other local organizations and individuals may not possess the knowledge and expertise in understanding the fast-changing functions and operations of a CERT team, we propose the governance of the centre to be done through two activities.

a) HKCERT will prepare an annual report on the achievement of the centre each year. The report will cover the incidents handled and activities carried out. The report will be posted on the HKCERT website so that the general public can understand the operations and activities performed, and provide suggestions. The report will also be submitted to OGCIO and presented to the HKPC industry cluster.

b) The management of HKCERT will meet with OGCIO twice a year, to discuss the operations and activities performed, and agree on the upcoming strategies and programmes of the centre.

5.2 Performance

The operations of a CERT centre will be adjusted according to the fast-changing information security and attack trends and the CERT services will be required in the event of emergency computer incidents. It is therefore very difficult to establish quantitative measures and measurement targets on the performance of a CERT centre. As the users of the services include also organizations from overseas and that the resolution of incidents involved a number of parties, it is not easy to obtain feedback on the satisfaction of service provided.

We propose the half-yearly meeting with OGCIO to be a good channel to evaluate the performance of HKCERT.

6. Future Plans

6.1 Areas of Work

With the increased sophistication of malware and phishing activities, many CERT teams around the world had established the capability to analyze malware and actively monitor the Internet on potential cyber threats. Many CERT teams have expanded the scope of services to include malware detection and analysis, cyber threat monitoring, and improved coordination with external parties. HKCERT need to enhance the existing services to include services identified below to cope with the latest development and to respond quickly to incidents.

a) Malware detection and analysis
  - To establish the technical environment to detect and analyze malware, in particular, those malware that targeted towards local organizations and users
  - To coordinate and liaise with other CERT teams in exchanging malware information, detection and analysis techniques and tools
  - To set up honeypots and honeynets to detect and analyze potential cyber attacks

b) Coordination and information exchange with global CERT teams on malware

c) Establishing A Cyber Threat Watch and Analysis System
  - To identify the approach, mode of operations, tools and partners on the establishment of the Cyber Threat Watch and Analysis System in Hong Kong
  - To plan and implement such a system in Hong Kong
  - To provide early warning and threat analysis reporting based on the findings and analysis results

d) Building up a closer working relationship with ISPs, information security solution and service providers

- To establish and agree with different ISPs on reporting and handling procedures so as to shorten the response time on the reported incidents
- To plan and coordinate to conduct a local drill

e) Incident Handling Systems and Techniques improvements

f) Promotion Campaign on the services of HKCERT

- To promote the services of HKCERT
- To promote the awareness of Information Security through industry associations

g) Incident Handling Capability Building

- To assist in building up the incident handling capabilities and establishing local CERT teams in large corporations
- To extend the coordination network to include critical infrastructure and to improve the communication with these organizations on potential threats and assistance in incident response and recovery actions

6.2 Resources and Expenses

This part is left blank intentionally

- END -