

The Telecoms InfoTechnology Forum

The Importance of Security Reviews



Presented by

**Mr. John Wong
Assistant Government Chief Information Officer**

27th March 2006

政府資訊科技總監辦公室
Office of the Government Chief Information Officer

1

Distinguished Guest, Ladies and Gentlemen,

Good Afternoon! I am pleased to be invited to speak at this forum today.

Security Challenges

- **ICT Use in Hong Kong Keeps Rising**
- **Cyber Attacks Also Becoming more Concerning to Users**
- **No Foolproof Solution to Information Security But Can Minimise Threats and Impacts**



2

Hong Kong has been receptive to the use of electronic means in communication and business with the highest PC and broadband penetration in the world. According to the Census & Statistics Department's (C&SD) Surveys Report published early this year, the number of Internet connection in households has risen from 1 million in 2001 to 1.5 million in 2005, representing a 50% increase. The Internet connection in business establishments rose from 37% in 2001 to 54% in 2005. The value of business receipts from selling goods, services or information through electronic means has recorded \$27 billion in 2004 which is a rise of 30% from \$21 billion in 2003. It is expected that the use of ICT and Internet in the business sector will continue to increase steadily in Hong Kong.

While ICT makes life easy and efficient for the users, it also provides opportunities to people with malicious intents to launch attacks to victims on the Internet. According to a recent report on security threat published in March 2006, on average 39 attacks involving 9,000 bot-infected computers were reported everyday and over 10,000 new viruses and worms were identified in the second half of 2005.

The paradigm of Internet communication and e-business is irreversible. What we can do is to ensure that we have the capability to protect, detect, react and recover from cyber threats.

Information Security Management

- **HKSAR Government's Information Security Management Framework Also Published for Public Reference**
- **Periodic Information Security Review Checks Health Status and Identifies Security Risks**
- **Take Follow Up Actions after the Review to Plug the Holes**

3

Although there is no foolproof solution for information security, it is possible to minimize the risk and impact of security incidents by establishing an information security management framework. Government has led by example, and developed comprehensive IT security policy and guidelines to be adopted by all Government departments. These include a Baseline IT Security Policy, IT Security Guidelines, Security Risk Assessment and Audit Guidelines, and Information Security Incident Handling Guidelines. These procedures and guidelines were developed with reference to international best practices, professional sources and are reviewed from time to time to reflect changes in technology and security threats.

Information security is not a static feature. Organisations should continuously monitor the performance of their information security measures as well as conduct regular assessment and review on their information systems to confirm the health condition of the information systems, data and networks as well as evaluate potential risks. Any identified loopholes should be plugged without delay.

Information security is about policy, processes, tools and people. A security review should cover high-risk areas such as the interfaces of the internal network with the Internet, the corporate procedures for handling classified data, and the protection measures at a computer center and user offices relating to the corporate objectives, business strategies and operations. Some threats may have significant impacts to the daily operations while others may have adverse effects on the business strategies. Depending on the vulnerability and impact analysis result, those risks that could affect the confidentiality, integrity or availability of

Example - WTO/MC6

- **We Did an Information Security Review, and**
 - **Assessed Various Components**
 - **Identified Possible Cyber Risks**
 - **Strengthened Weaknesses/Plugged Loopholes**
 - **Rehearsed Well Before the Event**
 - **Monitored & Responded to Cyber Security Issues/Incidents**
- **MC6 was successfully completed without cyber security problems**

4

I would like to mention how information security review had helped in our preparing for the World Trade Organisation's sixth Ministerial Conference (MC6) that was successfully held last December. Cyber security was one of the key concerns on the Government's agenda according to the past experience of other major international events. Besides enhancing the information security measures within Government and coordination among stakeholders of critical infrastructure, we conducted a quality assurance review on the relevant information security components such as the policy and guidelines, security measures, training, surveillance and incidents response capability, as well as common services, networks and e-Government services platform.

Without going into details of the process, I can tell you that as a result of the review we had improved our staff awareness, incidents handling procedures, business continuity plans, collaboration and co-operation with the Internet service providers, and others. As it turned out, the MC6 was successfully completed without many cyber security problems.

Finally, I want to emphasize to you that periodic information security review is a mandatory and on-going activity to fight against the ever-changing information security challenges.



Thank You!

5

Thank you.