

**DISCUSSION PAPER**  
**ADDRESSING INFORMATION SECURITY ISSUES**  
**IN THE HONG KONG SPECIAL ADMINISTRATIVE REGION**

**Prepared jointly by:**

(in alphabetic order)

Hong Kong Computer Society – Information Security Specialist Group  
Information Security and Forensics Society  
Information Systems Audit and Control Association – Hong Kong Chapter  
Information Systems Security Association – Hong Kong Chapter  
Professional Information Security Association

**Supported by:**

Office of Sin Chung Kai, Legislative Councillor (IT)

## **Introduction**

There has been growing concern over information security in Hong Kong, given the increasing number of security-related incidents reported by the media in recent years. In addition to the traditional viruses and hacking activities, the recent phishing scams and the nuisances caused by spamming have shaken public confidence in the security of IT products and services.

The purpose of this Discussion Paper is to raise the general awareness of information security in Hong Kong and to facilitate public discussion by highlighting the top ten information security issues and challenges that needs to be addressed by the HKSAR Government and the IT industry in the coming years.

A task force comprised of local information security professionals committed to shaping a better information security environment in Hong Kong was established in October 2004. The organizations (see Appendix 1 for more details) that they represent include:

- Hong Kong Computer Society – Information Security Specialist Group
- Information Security and Forensics Society
- Information Systems Audit and Control Association – Hong Kong Chapter
- Information Systems Security Association – Hong Kong Chapter
- Professional Information Security Association
- Office of Sin Chung Kai, Legislative Councillor (IT)

## **Issue 1 – Role of Government**

Before addressing any specific information security issues, the task force believes that it is important to clarify the role of the HKSAR Government in building a secure IT environment for both the local community and overseas investors. While the task force agrees that organizations/industries themselves should be responsible for examining the importance of information security to their business objectives, and to consider appropriate information security measures tailored to their specific needs, we believe that the Government should take a leading role in the co-ordination and management of critical infrastructure, of which the information infrastructure is one of the essential components. The security of critical information infrastructure may involve multiple government bureaux and departments (e.g. OGCIO, Security Bureau, Education and Manpower Bureau), other related public institutions (e.g. HKCERT, HKMA, OFTA, HKIX, HKIRC), private businesses (e.g. ISPs, cable providers, information security vendors), professional bodies and trade organizations.

## **Issue 2 – Communication and Consultation**

In the Digital 21 Strategy, HKSAR Government has clearly indicated its commitment to maintain a secure environment in the promotion and development of IT. While this is certainly welcomed by the industry and the general public, we see much room for improvement in the communication and consultation process with the industry, including professional bodies and trade organizations. We have attended social gatherings in the past organized jointly by the various law enforcement agencies under the Security Bureau. These gatherings were useful in establishing connections with key players in the industry, but lacking specific focus on tackling real issues encountered by the public. We recommend a more formal Information Security Committee be established with representatives from leading information security professional bodies to supervise the development of information security policies and action plans in Hong Kong. The vision of the Committee is to ensure that information security of critical information infrastructure is managed effectively and in a co-ordinated fashion, and to ensure that clear policies and appropriate priorities are established for the long-term development of information security in Hong Kong. The Committee should establish specific goals and objectives, and should meet on a regular basis.

We believe that the method of public consultation is also important in facilitating the building of consensus and unity within the community. The Government should continue to demonstrate openness and transparency throughout the public consultation period.

## **Issue 3 – IT Governance and Information Security Standards**

The task force believes that it is important to understand that information security standards are ultimately applied in a business context, and therefore need to be closely linked to how IT is managed and governed. The need for security standards therefore must not be viewed in isolation, and must be considered in the context of IT Governance, given the role of Hong Kong as an international financial centre, and the heavy use of, and reliance on, information technology by corporations and citizens.

In this context, we recommend that the Government should:

- Work with appropriate regulating bodies and associations (e.g. Securities and Futures Commission, Hong Kong Exchanges and Clearing Ltd., Hong Kong Monetary Authority, Office of the Commissioner of Insurance, Hong Kong Institute of Certified Public Accountants, Hong Kong Institute of Directors) to promote the concept of IT Governance as

an integral part of Corporate Governance;

- Accept and adopt suitable internationally recognized framework and standards (e.g. COBIT, ISO17799) supporting IT Governance and Information Security; and
- Evaluate the feasibility for establishing mandatory minimum standards and guidelines for critical infrastructure to conform to IT Governance and Information Security requirements.

#### **Issue 4 - Security awareness (general public), training and education**

Although training and education opportunities are widely available in Hong Kong, we found that most of them are designed for IT professionals and information security practitioners, and not suitable for SMEs and the general public. General awareness initiatives on how to take preventive measures to protect an individual or organization's sensitive/critical information and the way to react to information security related issues in daily life are considered to be inadequate.

We recommend that the Government should:

- Implant basic information security concepts through ethical education in primary and secondary schools. This can be achieved by including cyber ethics in the school curriculums, and hence will provide an established path for every citizen to build up a security sense and accountability from an early age.
- Organize campaigns targeted to the general public, on a regular basis, to promote the need and importance of protecting information security assets. This can be achieved through producing more TV or radio programme series.

#### **Issue 5 - Certification (professional, organizations, products)**

Hong Kong is one of the leading cities in terms of concentration of internationally certified information security professionals. IT professionals in Hong Kong are keen to obtain IS certifications and there is a healthy supply of certified information security practitioners to cater for the market's need. They are valuable assets for Hong Kong towards its migration to a knowledge-based economy. However, in recent years, these practitioners are pressed continually to spend more of their own time and money in acquiring new skills to fulfill the demand from stringent professional requirements of the fast-changing environment. We suggest that the Government should take appropriate measures to relieve their pressure, for example, by including selected information security education programs into education funding schemes (e.g. CEF and ITF).

The task force also noticed that most organizations in Hong Kong are not keen to adopt industry recognized IT governance and information security standards such as COBIT and ISO17799, unlike other countries in the region (e.g. Japan and Korea). The advancement of other countries in the region is primarily the result of requirements imposed by the government through regulatory bodies. We strongly believe that the HKSAR Government should consider taking similar approach to create the demand for certification. From a long-term perspective, and similar to the ISO quality standards, increasing the number of certified information security organizations in Hong Kong will increase their competitiveness in the region, and help to maintain Hong Kong's leadership position in attracting overseas investors.

### **Issue 6 - Information Security Research and Development**

With globalization and technological revolution taking place around the world, Hong Kong must transform into a knowledge-based society in order to maintain a competitive edge in the region. To meet this challenge, information and knowledge are critical. Information security research and development must be encouraged to ensure that local information security professionals have the skills and knowledge to build world class security solutions. This will not only help to protect our information assets but also facilitate local companies to take a lead in the region and grow in the global market. The R & D effort should encompass not only information security products but also education, methodology, framework and standards. While the existing programs under the Innovation and Technology Fund (ITF) addresses part of the issues noted above, the following suggestions should be considered by the Government in order to improve information security R & D efforts and results in Hong Kong:

- Information security R & D should be explicitly included as one of the IT areas within the Applied Science and Technology Research Institute (ASTRI) of the ITF.
- An Information Security Committee (see related discussion in issue 2) should be established to identify appropriate R & D initiatives.
- It is necessary to establish effective communication channels with the defense and security industries in the mainland such that HK enterprises can participate in appropriate R & D initiatives for products, education, methodology, framework and standards.

## **Issue 7 – Collaboration with Mainland China**

In addition to being a major global financial centre, one of the competitive strengths of Hong Kong is in information technology especially in the areas of **Information Security (IS)**. At a time when investment growth in Mainland China is accelerating and the reliance on information technology is growing, Hong Kong companies in the IS industry can gain access to the massive China market by leveraging on their strength. IS can serve as a ‘Bridge’ to add value to professional and business transactions between Hong Kong and Mainland China, and to enhance the prosperity of both parties.

We recommend that the Government should:

- Facilitate the enabling of IS consultancy and training assignments to be conducted in China by HK’s IS professionals, with special concession on withholding tax, fee settlement and remittance procedures, in consideration of the nature of these professional services being a skill and know-how imported to China which supplement the current IS skill shortage in the Mainland, and directly assist China enterprises to strengthen their competitive advantage in view of the competition expected after China’s entry to WTO and compliance to international business practices of local enterprises. These concessions can initially be rolled out in the major cities such as Beijing, Shanghai, Guangzhou and Shenzhen.
- Discuss and reach agreement with the Central Government in Mainland China to enable the set-up of Chapters or local representative offices for international IS professional associations in the Mainland, with due consideration to proven track records and history in HK and internationally. This can enhance the training, education, and networking of the IS professionals between HK and Mainland China in the private sector, and will accelerate the exchange of knowledge, and positively enhance the business growth of IS enterprises in both Hong Kong and Mainland China.
- Facilitate a platform on which Mainland IS projects can be opened to tendering by HK IT companies. This will enable the expertise of HK’s IS/IT industries to be utilized upon accelerating business exchange between HK and Mainland in the areas of Information Security, increasing the economic prosperity of HK, whilst at the same time enabling and accelerating Mainland’s IS industry development in a legitimate manner with due protection and utilization of IP rights.
- Extend the current special travel scheme for individual visitors from Mainland China to make it more convenient for individuals to acquire visas to visit HK for attending professional training, seminars/conferences, and sitting for professional examinations.

## **Issue 8 – Computer Forensics**

With the growth trend of electronic and internet based crimes, Information Technology (IT) forensics investigation procedures need to be established for handling digital evidence. Although some Information Technology related Ordinances have been enacted in Hong Kong, there are currently no common forensics investigation practices, digital evidence seizure or collection standards that have been established and commonly adopted by the HKSAR Government, as in Australia, Canada, US and UK, where different law enforcement teams and private sectors collect digital evidence based on different code of practices. In addition, computer forensics laboratories for collecting and analyzing digital evidence are only being set up within some law enforcement agencies. No standardized investigation tools, procedures and knowledge base have been established across these laboratories. It should be noted that there are very few computer forensics facilities or laboratories established for providing services to suspects/defendants.

We recommend that the Government should consider the following:

- A common computer forensics investigation procedures and standards should be developed or adopted by the law enforcement team and private sectors under the Hong Kong legal systems. These procedures and standards should be endorsed as the framework for Hong Kong computer forensics investigations.
- A standardized professional examination commonly accepted by the Hong Kong legal systems, law enforcement and IT security industry should be established.
- Independent computer forensics laboratories should be set up to provide computer forensics investigation and verification services in order to ensure that sufficient legal support is available to both the plaintiff and defendant.
- The HKSAR Government should encourage forensics technology development in Hong Kong by supporting the research and development of computer forensics procedures and products, thereby establishing Hong Kong as a leader in this area.

## **Issue 9 - Business Continuity and Incident Response**

A single incident within the critical information infrastructure can adversely impact the survivability of the whole infrastructure. Recent examples are the SQL Slammer worm outbreak in 2003, the unavailability of the HKIX and the HKIRC in 2004, which had greatly impacted the local internet services as a whole. The Government should play a more active role in supervising the continuity and response capability in relation to security incidents of the overall

infrastructure. We believe that the first thing is to have a clear definition of the critical information infrastructure for Hong Kong.

In terms of "Business Continuity", the Government should identify deficiencies in the continuity capability management system and propose to each responsible organization a roadmap for improvement. In the long run, it is necessary to work with the related organizations to develop a set of minimum standards for continuity requirement and to define service level and response time to report acute incidents to the Government.

For "Incident Response", we recommend that the HKSAR Government should build a network and attack monitoring system for the city to provide pre-attack indicators before the attack has built up to a harmful momentum. These systems have been successful in the global perspective (e.g. Internet Storm Centre) and Asia Pacific economic entities (both Korea CERT and Japan CERT have implemented and China CERT is in the process of building one). In addition to developing the monitoring capability, we also propose to build up an effective incident response coordination framework for large scale cyber attacks.

#### **Issue 10 – New and emerging technologies**

We have all seen the rapid pace of technological advancement. New products and new services with innovative features continue to fuel growth and improve our ways of life. Examples include 3G, wireless LAN, instant messaging, Internet shopping, Internet banking and smart ID cards. All these products and services are known to have weaknesses that have been exploited and misused. As new and emerging technologies are introduced, new threats and vulnerabilities are surely to arise. These weaknesses have caused the industry billions of dollars of damages each year and there is no sign of slowing down. Proper risk assessment and risk management should be incorporated throughout the product life-cycle of new products and services so that risks could be managed and the impact of damages could be minimized.

We recommend that the Government should empower an Information Security Committee to:

- Identify new products and new services that may have an impact to the general public or the industries.
- Form working groups to assess the threats and risks related to the new information security products and services so that appropriate policies, standards, and control measures could be suggested to relevant parties with an objective of minimizing risks and impact.

## **The way forward**

This discussion paper has attempted to highlight the most significant information security issues and some of the current thoughts of the local practitioners. It certainly does not, and should not, end here. We believe that the best way to move forward to address these issues and challenges will be for the HKSAR Government to take a proactive approach by establishing an Information Security Committee as suggested in this paper. With the HKSAR Government, regulating bodies, professional organizations, and trade associations working together, we are confident that a better information security environment will be created in Hong Kong.

## **Appendix 1 – Professional Information Security Organizations in Hong Kong**

### **Hong Kong Computer Society – Information Security Specialist Group**

The Hong Kong Computer Society (HKCS, [www.hkcs.org.hk](http://www.hkcs.org.hk)) was founded in 1970 and is a non-profit professional institution for the field of information technology. The primary objectives of the Society are to promote IT knowledge and maintaining a code of conduct for its members. It has been providing valuable service and support to the IT community, including individual practitioners, employers of IT staff and the general public in Hong Kong and the Asia-Pacific Region for over 30 years.

The mission of the Hong Kong Computer Society is to accelerate the understanding, adoption, use and widespread acceptance of Information Technology (IT) through educational programs, advocacy, industry relations and by bringing together, in an open forum, leading users and technologists from both the public and private sectors.

The Information Security Specialist Group (ISSG) was formed in 2000 by a group of leading professional information security practitioners in Hong Kong. The ISSG is operating under the Hong Kong Computer Society with the following specialized objectives:

- (a) To promote information security;
- (b) To promote the use and development of information security technologies and applications; and
- (c) To provide a forum for the exchange of information and experience in the area of information security.

## **Information Security and Forensics Society**

Information Security and Forensics Society (ISFS, [www.isfs.org.hk](http://www.isfs.org.hk)) was registered under the Hong Kong Societies Ordinance in May 2000. Our mission is to advocate and enforce professionalism, integrity and innovation in Information Security and Computer Forensics in Hong Kong and the surrounding region.

### **Goals**

1. to regulate and standardize the practice of information security and forensics professionals;
2. to conduct examinations and act in such other manner as may be necessary to ascertain whether persons are qualified to be admitted to register as an information security and forensics professional;
3. to encourage the study of information security and forensics by holding regular training courses and seminars;
4. to promote public awareness of information security and forensics.

### **Vision**

To be one of the leading pioneers in establishing the science and professional ethics in information security and computer forensics.

### **Mission**

To advocate and enforce professionalism, integrity and innovation in information security and computer forensics.

### **Strategic Objectives**

1. To develop information security and forensics with a view to maintaining a premier environment for the widest application of information technology.
2. To share the knowledge of information security and forensics and to deter exploitation of information technology for illegitimate purposes.
3. To help establish the scientific discipline of information forensics and digital evidence with local and international professional bodies.
4. To develop an internationally recognized training and accreditation programme for information security and forensics professionals.

## **Information Systems Audit and Control Association – Hong Kong Chapter**

The Information Systems Audit and Control Association (ISACA) was founded in 1969. It is a globally recognized leader in IT governance, control and assurance organization. Its mission is, through worldwide leadership, to enhance recognition of the IS audit and control profession through the advancement of standards and practices, education and certification. It assists IT governance, control and assurance stakeholders to deal with IT management, IT risk and IT process, and their interaction with corporate governance, corporate management, corporate risks and corporate processes. ISACA provides value through various services, such as research, standards, information, education, certification, and professional advocacy. The Association helps IS audit, control and security professionals focus not only on IT, IT risks and security issues, but also on the relationship between IT and the business, business processes and business risks.

ISACA has over 44,000 members worldwide and administers the globally respected Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) certification programmes.

ISACA is represented in Hong Kong through a local Chapter which has over 1,200 members and offers the following services to its members and the public:

- Providing opportunities for information exchange and networking through regular chapter meetings.
- Organising continuing education programmes, and review courses for the CISA examination.
- Conducting research and issuing publications.
- Providing opportunities for the practice of leadership on local boards and committees.
- Directing views and commenting on legislation that impacts the profession and local business community.

Hong Kong Chapter celebrated its 20<sup>th</sup> Anniversary in 2002, and has received the Best Chapter Award, the Largest Chapter Award, and the Gold Website Award in recent years.

For more information on the Association's products and services, please visit the Hong Kong Chapter website at <http://www.isaca.org.hk>, ISACA International website at <http://www.isaca.org>, or e-mail to the Hong Kong Chapter President at [president@isaca.org.hk](mailto:president@isaca.org.hk).

## **Information Systems Security Association – Hong Kong Chapter**

The Information Systems Security Association (ISSA) is a not-for-profit, international organization of information security professionals and practitioners. The Association provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members. ISSA members include practitioners at all levels of the security field in a broad range of industries, such as communications, education, healthcare, manufacturing, financial and government. The Association has an international communications network developed throughout the industry and is focused on maintaining its position as The Global Voice of Information Security.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved.

The ISSA has 95 Chapters in 22 countries with over 10,000 members worldwide. The Hong Kong Chapter was founded in 2003 with members consisting of information security professionals and practitioners from a broad range of industries.

## **Professional Information Security Association**

Professional Information Security Association (PISA, <http://www.pisa.org.hk> ) is a not-for-profit organization founded in 2001 for local information security professionals. We have the vision to be the prominent body of professional information security practitioners, and utilize our expertise and knowledge to help bring prosperity to the society in the Information Age.

Our missions are:

- to facilitate knowledge and information sharing among the PISA members
- to promote the highest quality of technical and ethical standards to the information security profession
- to promote best-practices in information security control
- to promote security awareness to the IT industry and general public in Hong Kong
- to be the de facto representative body of local information security professionals