

Hong Kong Information Security Annual Survey

Conducted jointly by

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

Introduction

This survey is conducted by the working group on information security from April 20 to June 30, 2005. It targets the Hong Kong IT environment. This is the first time the survey is conducted and it will be conducted periodically in future.

This survey addresses the major IT security concerns in the IT industry from the information security practitioners (or professions) in Hong Kong. All respondents of this survey are security professions in Hong Kong.

In Hong Kong, IT security shall be treated seriously because core businesses and critical infrastructures are relying on IT systems and communications. Hong Kong would suffer from major financial lost or even life lost if major security incidents ever happened. Therefore, we would like to assess the security issues and the road ahead for the IT security development in Hong Kong through this survey. In addition, we would like to arouse the security awareness in the IT industry or public with this survey.

The issues assessed in this survey include:

- 1) Role of Government in Information Security
- 2) IT Governance and IS Standard
Information Security Awareness
- 3) Certification of quality of the IS workforce
Research and Development
- 4) Collaboration with Mainland
- 5) Computer Forensics and Law Enforcement
- 6) Critical Information Infrastructure Continuity and Incident Response

Key Findings

Around 170 respondents participate and response to the survey questionnaires. Majority of these respondents are members of the 5 security professional organizations or information security professions.

Based on the survey results, it was observed that the IS practitioners and IT industry professions agreed that HKSAR government has not put sufficient attention in developing IS industry and environment in HK. IS practitioners also expressed that there are insufficient communications between IS practitioners with HKSAR Government in developing IS policies and strategies.

IS practitioners also highlighted that IT Governance and IS industrial standards have not been adopted widely as compared with other regional economies. Some possible reasons are insufficient IS awareness in public community, insufficient supply of qualified manpower in the IS field and insufficient R&D activities in the local IS industry.

According to the survey results, in the ever changing IT environment, the following IS concerns are considerably important to HK IT industry and IS practitioners:

- Inadequate support to local IS industry to tap into Mainland IS market
- Insufficient computer forensics facilities/resources to cope with current growth of computer-related crime
- Unclear plan in establishing a highly continuous and robust critical information infrastructure against information security attacks
- Insufficient input from industry and government on exploring security threats of new and emerging technologies

Based on the comments on most concerned information security areas from the survey, it is obvious that IS practitioners the list of top 10 IS challenges to the government and IS industry composed by the working group highlights the most concerned areas of IS practitioners.

In order to be competitive in Information Security area when compared to other regional economies, IS practitioners highlighted that Hong Kong government and IS industry should put in more resources to support the IS industry and actively response to all the 10 proposed information security areas of concern especially in promoting and facilitating the adoption of IT governance and IS standards in public and private sectors. Government should play an active role in solving these 10 concern areas.

Detailed Analysis

Role of Government in Information Security

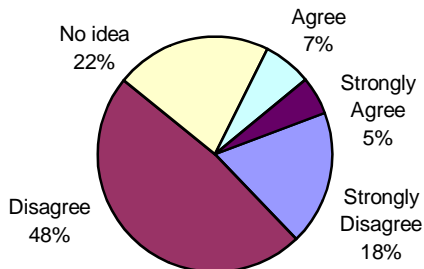


Figure 1. Is there a comprehensive and long-term IS policy in HK?

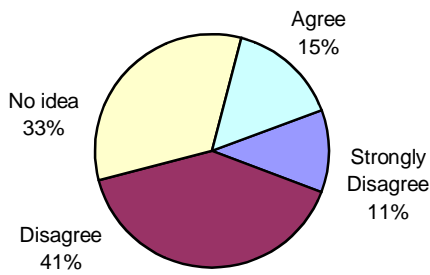


Figure 2. Is HK is currently competitive in IS when compared to other regional economies?

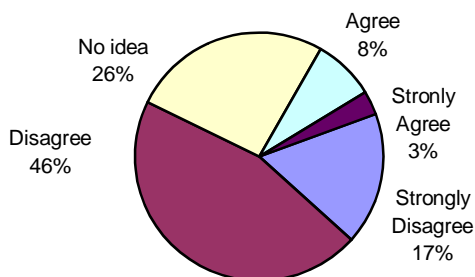


Figure 3. Is HKSAR playing a leading role in coordination and management of critical information infrastructure?

We are concerned about the role of HKSAR Government in promoting the IS in IT industry. The role of Government is important in promoting IS in other countries.

Figure 1 shows that most of the respondents (66%) do not think that a comprehensive and long-term IS policy exists in HK. Only a minor group (12%) agrees that there is an IS policy in HK.

Among the respondents, only 15% of them think that HK is competitive in the region while 52% believe uncompetitive, as shown in Figure 2.

Regarding the security of critical information infrastructure, around 63% of them do not believe HKSAR is taking the role to coordinate and manage it properly and only 11% of them think that HKSAR is doing the job right.

From these results, it can be concluded that the respondents think that HK should establish a long-term comprehensive IS policy to improve its competitiveness in the region. In addition, HKSAR should take a more active role to lead the IS development in protecting the critical information infrastructure.

Communication and Consultation

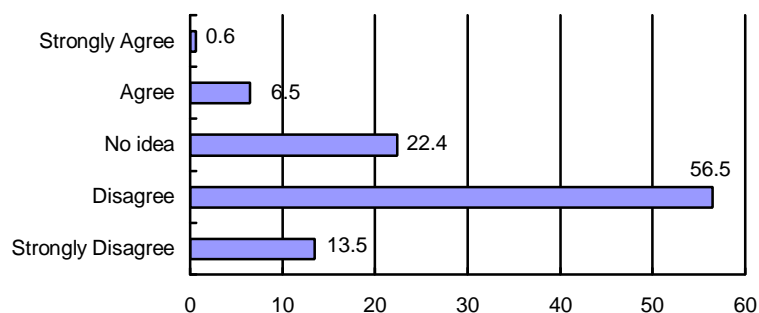


Figure 4. Can the public see a clear division of labor and collaboration among HKSAR departments?

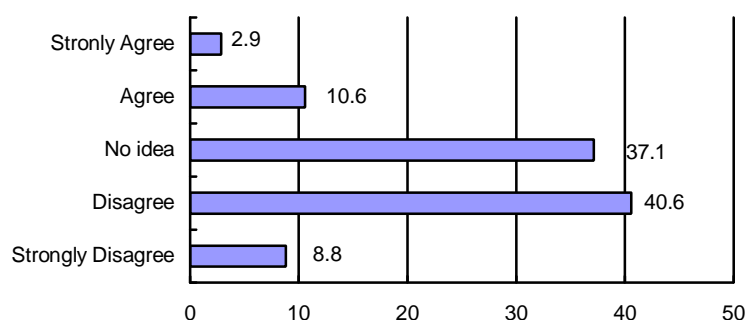


Figure 5. Are opinions from IS experts effectively communicated to HKSAR in the development of IS policies and strategies.

The respondents, in general (60%), do not believe the public can see a clear division of labor in HKSAR departments to promote IS in HK.

Also, about half of the respondents do not believe that the opinions from IS experts can effectively communicate to HKSAR in the development of IS policies and strategies; only 13.5% of them believe the opinions are properly communicated.

From these results, HKSAR should have a clear IS strategy and plan so that the division of labor inside HKSAR is properly assigned. As a result, the opinions from IS experts can be effectively communicated to HKSAR in the preparation of IS policies and strategies.

IT Governance and IS Standard

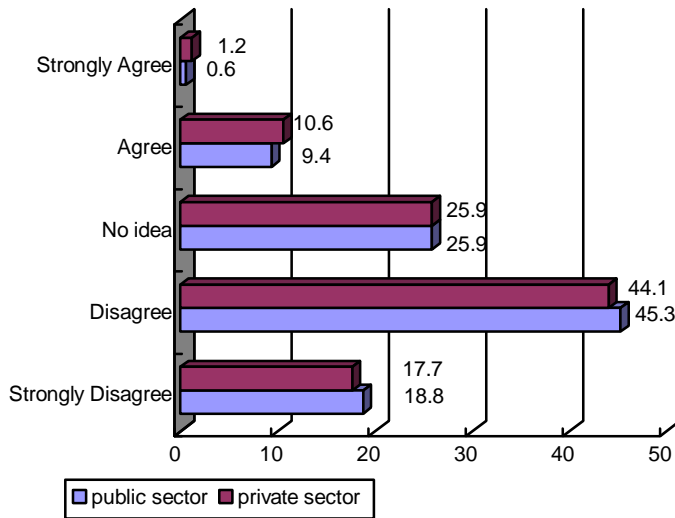


Figure 6. Are standards for IT governance and IS well deployed in local public and private sectors?

Promoting IT governance in the public and private sectors should enhance the security of the organizations.

From the results of the survey, IT governance is not regarded as well deployed in both public and private sectors – over 60% of the respondents believe so. Only around 10% of them share the same opinion that it is well deployed in HK.

We do not have the degree of deployment in other regions. Therefore, we cannot determine the status of IT governance in HK. Nevertheless, we believe that IT governance should be promoted in HK to enhance IT security and also the overall IT management. This shall be beneficial to long-term development of HK IT industry.

Information Security Awareness

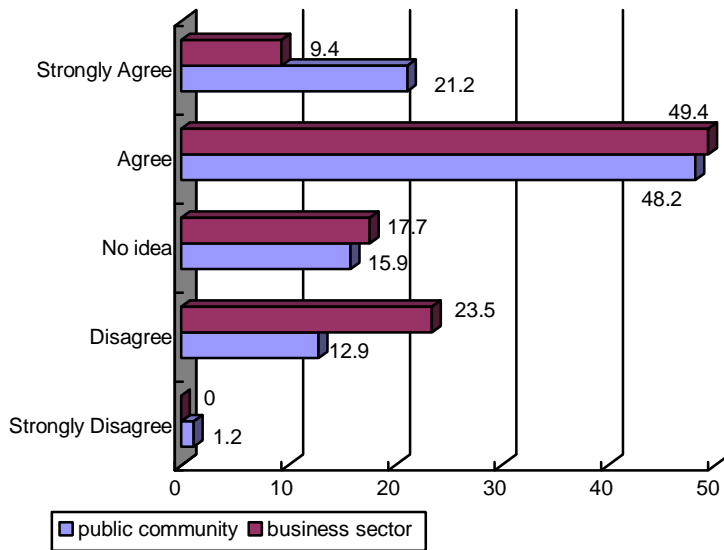


Figure 7. Does IS awareness in the business sector and public community remain at low level?

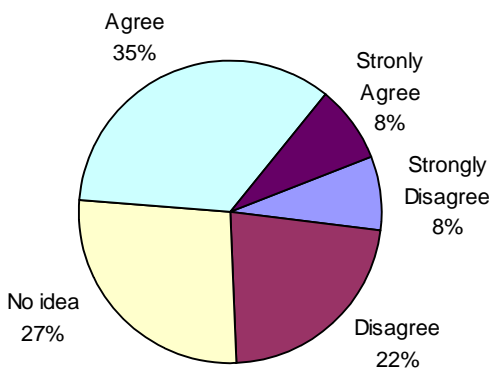


Figure 8. Has my organization provided sufficient IS awareness training to staff?

The security awareness of an organization is a good indicator for the effectiveness of security protection in that organization.

Figure 7 shows that, in general, the respondents regard the security awareness in business sector is better than that of public community.

Around 70% of them think that the security awareness of the public is still low while only 14% think it is proper.

However, around 23.5% regard the security awareness is proper in business sector. Nevertheless, around 59% of them still consider the awareness is low in this sector.

Although many respondents consider security awareness in business sector is low, there are still 43% of them agree that their organizations have provided sufficient security awareness training to them. Only 29% of them consider their awareness training not enough.

From these results, a more effective security awareness training program should be developed to enhance the security awareness in the business center and the public community.

This matches the collective ideas of the working group on IS awareness requirement. The working group thinks that more training resources should be allocated to IS awareness training in primary and secondary schools in their general education courses.

Certification of quality of the IS workforce Research and Development

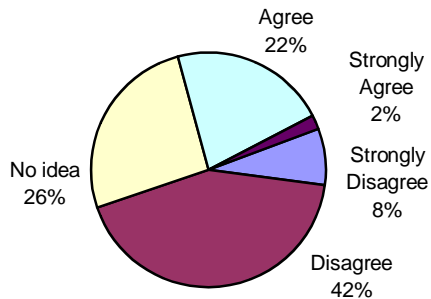


Figure 9. Is there sufficient supply of qualified manpower in the field of IS?

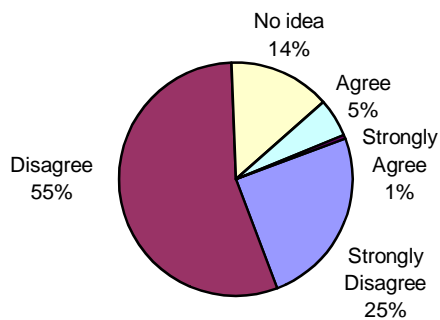


Figure 10. Has HKSAR provided good incentives for the workforce to develop IS expertise?

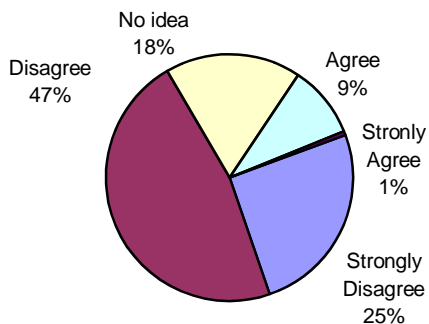


Figure 11. Has HKSAR enforced the adoption of IS professional certification?

Qualified security practitioners are essential to the IS development in HK.

In this survey, as shown in Figure 9, more respondents (50%) consider the qualified security staff is insufficient in HK. Still, 24% of them believe there are enough qualified security staff in HK.

However, there is a majority (80%) believing HKSAR has not provided good incentives for the workforce to develop IS expertise. In addition, many respondents (72%) disagree that HKSAR has enforced the adoption of IS professional certification.

As a conclusion for this issue, a program should be devised to initiate the development of IS expertise and to promote the adoption of security certification in HK.

Research and Development

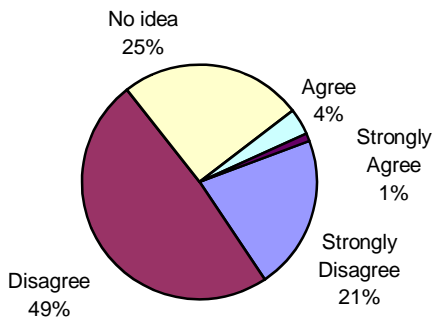


Figure 12. Are existing resources and support adequate for local R&D in IS field?

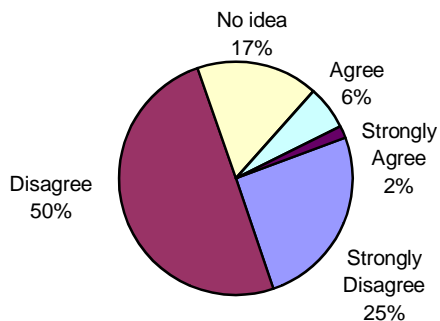


Figure 13. Are there sufficient R&D activities in local IS field?

R&D of IS field is believed to be very insufficient in this survey.

Most of the respondents (70%) do not believe enough resource and support are allocated for local R&D in IS field. Only a few of them (5%) believe so. Therefore, not surprisingly, 75% of them consider there are insufficient R&D activities in local IS field while around 8% consider sufficient.

Therefore, we believe a program should be prepared to promote the R&D activities in local IS field in HK. Otherwise, HK may lose its competitiveness in IT security in the region.

Collaboration with Mainland China

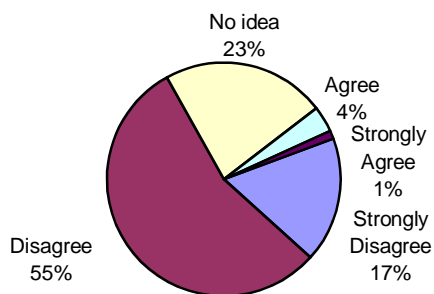


Figure 14. Has Government provide adequate support to local IS industry to tap into the Mainland markets?

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 in Information Security.

However, over 70% of the respondents considered that the HKSAR government has not provided adequate support to local IS industry to tap into the Mainland markets while only 5% considered adequate.

Thus, we believed the HKSAR government can help by liaising and reaching agreement with China so that Hong Kong's IS consultancy and training assignments can be conducted on the mainland, with special concession for tax treatment, fee settlement and remittance procedures.

Computer Forensics and Law Enforcement

With the growth trend of electronic and Internet based crimes, Information Technology (IT) forensics investigation procedures need to be established for handling digital evidence.

In this survey, as shown in Figure 15 and Figure 16, slightly more than 50% of the respondents considered that Hong Kong has not provided sufficient computer forensics facilities to handle forensics data and law to combat against computer-related crime.

Therefore, our working group agrees that HKSAR government should develop a common forensics investigation procedure and standards to facilitate our law enforcement agencies in handling digital evidence.

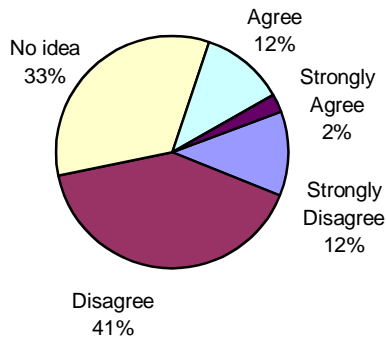


Figure 15. Are there sufficient computer forensics facilities in Hong Kong?

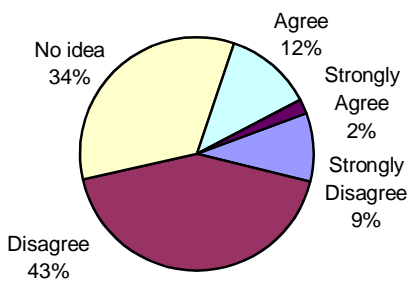


Figure 16. Are there sufficient law to combat computer-related crime?

Critical Information Infrastructure Continuity and Incident Response

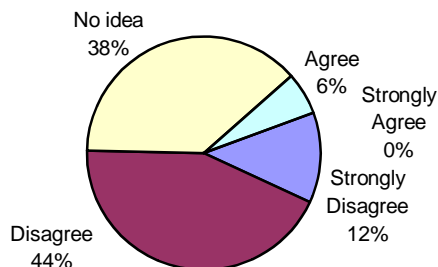


Figure 17. Is the improvement roadmap of critical information infrastructure been defined?

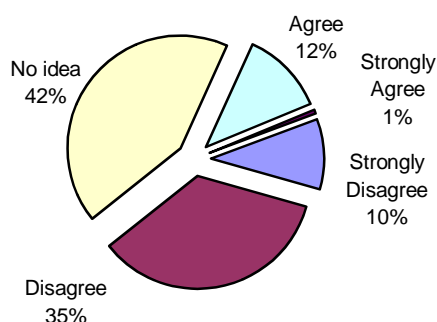


Figure 18. Has business continuity arrangement of Internet infrastructure been controlled by HKSAR government?

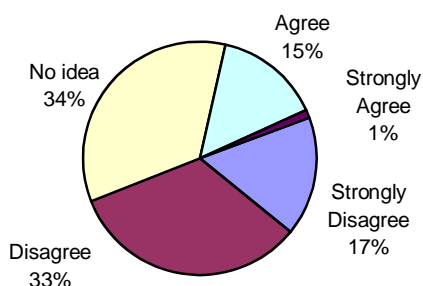


Figure 19. Are current Internet infrastructure of Hong Kong capable of handling large scale information security attacks?

Without any business continuity and incident response planning, a single incident within our critical information infrastructure can adversely impact the survivability of the whole infrastructure similar to virus outbreak in 2003, and unavailability of the HKIX and the HKIRC in 2004.

Although critical information infrastructure continuity planning are considerably important, over 55% of the respondents believed that improvement roadmap of critical information infrastructure has not been defined and only around 13% of the respondents think that business continuity arrangement of Internet infrastructure has been controlled by HKSAR government

As shown in Figure 19, around half of the respondents believed that, with current Internet infrastructure, Hong Kong is not capable of handling large scale information security attacks.

Thus the working group believes that HKSAR government should identify deficiencies in the continuity capability management system and establish an effective incident response coordination framework in order to protect our critical infrastructure from large-scale attacks.

New and Emerging Technologies

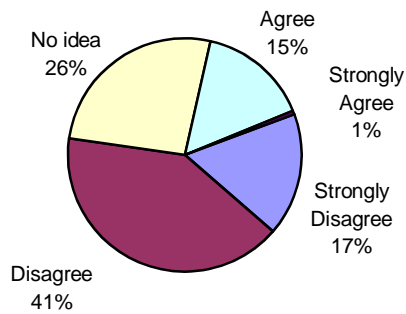


Figure 20. Has government been active in gathering input on security threats of new and emerging technologies?

New products and new services continue to change and affect our ways of life. As new technologies are introduced, new threats and vulnerabilities are arising.

As shown in Figure 20, around 58% of IS practitioners believed that HKSAR government has not actively gathered input on security threats on new and emerging technologies.

Therefore, we proposed that our government should work with the IS industry to identify appropriate policies and control measures to address risks arising from emerging technologies.

Overall Comment

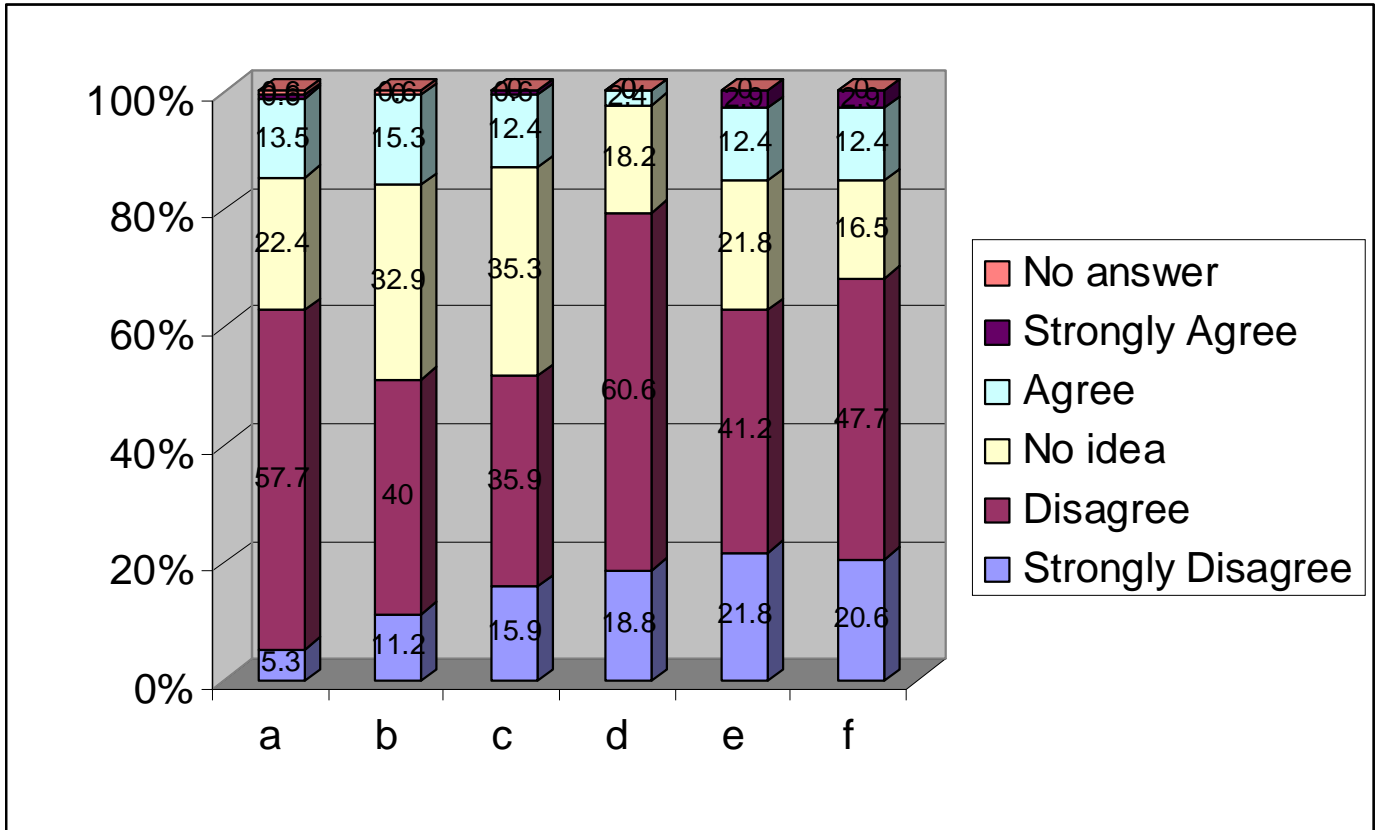


Figure 21. The overall comments of IS in Hong Kong. A) Is Information Security development in Hong Kong satisfactory? B) Is Hong Kong currently competitive in IS when compared to other regional economies? C) Five years later, will Hong Kong be competitive in IS when compared to other regional economies? D) Are resources currently allocated by the government to IS development in Hong Kong enough? E) Is Information Security threat to Hong Kong business low? F) Is Information Security threat to Hong Kong home users low?

In general, over 60% of the respondents are not satisfied with Information Security development in Hong Kong. The main reason is outlined by the responses of column d of Figure 21 – insufficient resources being allocated by HKSAR government to IS development (over 75% of IS practitioners response).

As Information Security threats to Hong Kong business as well as Hong Kong home users are not considered to be low as highlighted in sub-question (e) and (f), over 50% of the IS practitioners believed that Hong Kong is currently not as competitive in IS when compared to other regional economies. Without any change in IS development support by HKSAR government, around 50% of the IS practitioners also believed that Hong Kong will not be as competitive in IS when compared to other regional economies.

Most Concerned Information Security Areas

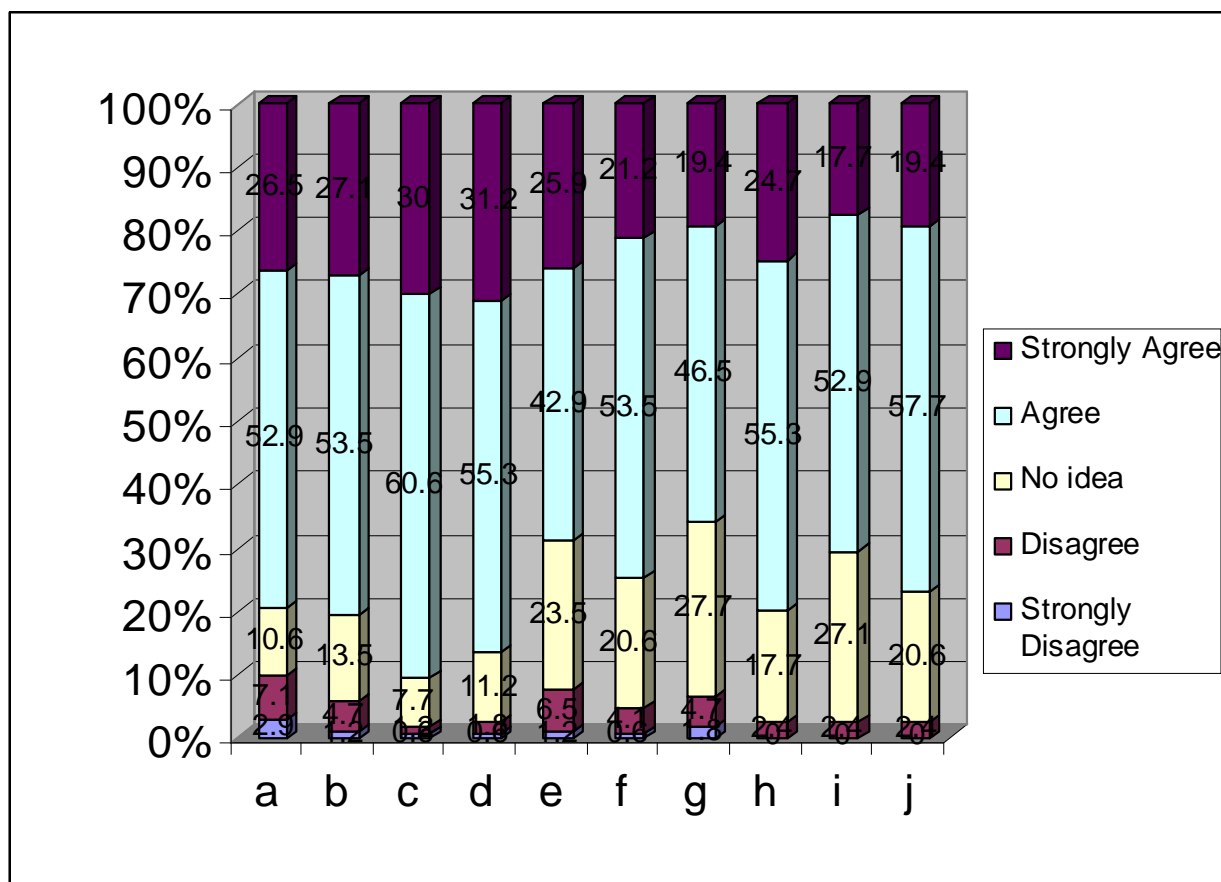


Figure 22. Which of the following information security areas of Hong Kong requires more development? A) Should Government play a more active role in IS? B) Should an Information Security Committee be setup across information security industry? C) Should IT governance and IS standards be promoted and adopted in public and private sector? D) Should IS awareness in the community be promoted? E) Should certification of the IS workforce qualifications be enforced? F) Should more resources to IS-related Research & Development be allocated? G) Should local IS industry to tap the growing Mainland market support be provided? H) Should business continuity planning and incident response capabilities of critical information infrastructure of Hong Kong be improved? I) Should computer forensics standards be adopted in Hong Kong? J) Should mechanism to gather opinions to assessing risks for new and emerging technologies be established?

In early January 2005, the working group outlined the top 10 IS challenges where HKSAR government and IS industry should address.

According to Figure 22, over 75% of the IS practitioners agreed that the top 10 listed IS challenges are considered to the information security areas of Hong Kong that requires more development.

Among all the development areas, IS practitioners agree that the following challenges are the top three areas of Hong Kong that requires more development:

- IT Governance and IS standards should be promoted and adopted in public and private sectors (over 90%)
- IS awareness in community should be promoted (around 86%)
- Information Security Committee should be setup across information security industry (around 80%)