ERIA Research Project Report 2008

No. 3-1

Strengthening Information Security in the Business Sector

Edited by

Dr. Komain Pibulyarojana

March 2009

Table of Contents

I. Background and Objectives

The economy in Asia (ASEAN + 6) has been rapidly developing and has been sustained by an increase in direct investment in the region and expansion of Economic Partnership Agreements (EPA). As a qualitative shift, the economy in the region has been moving toward a knowledge-based economy with the growth of high value-added industries.

These changes in the economy resulted from individual enterprise activities, while affecting those very same activities. Seen from the viewpoint of enterprise activities, the generalization of outsourcing, progress of cross-border technology transfer and progress of knowledge transfer, and the construction of the global supply chain support these changes and development.

Consolidating the development of Asia requires constructing a more advanced cross-border common infrastructure suitable for a knowledge-based economy and appropriate for the knowledge-based economy era. As part of this effort, it is important to invest in enterprise information security and to ensure the industrial policies of the region.

In order to promote further business outsourcing and foreign direct investment in Asia, a secure business environment needs to be created. For that purpose, it is essential to motivate each company to understand the importance of information security measures and take action.

For each company it is often difficult to fully grasp the information security level they should reach. In Japan, in order to establish and promote the idea of information security governance, the *Information Security Management Benchmark (ISM benchmark)* was developed as a self-check tool for organizations with which users can compare their security level with others. Three years have passed since this benchmark was released, and many organizations have used it.

In this project, we share the point of view and experience with other countries in Asia and develop a common information security management benchmark, which also takes the original situation of each country into account. Through the promotion of this benchmark, we aim to strengthen the information security measures of businesses in Asia.

II. Overview of the Research

Through this research, including two workshops, we studied the development of the common information security management benchmark (common ISM benchmark) in Asian countries. At first, we analyzed how the establishment of information security would affect the Asian economy and enterprise management in Asian countries. In addition, we also studied the role of the common ISM benchmark with regard to the impact (III-1) on the Asian economy and enterprise management.

We then studied the conditions and challenges of enterprise information security measures in Asia. Furthermore, we considered the requirements for the common ISM benchmark by applying the ISM benchmark developed by the METI (Ministry of Economy, Trade and Industry) and operated by IPA (Information-Technology Promotion Agency) in Japan and then evaluated the benchmark (III-2).

Last, we analyzed the results of the trial and evaluation and proposed visions and goals for establishing the common ISM benchmark. In addition, we described the challenges to establishing the common ISM benchmark (III-3).

Workshops

	Date	Place	Agenda
1st	December 25, 2008	Tokyo	・Presentation of the current status of information security in the business sector from each country.
2nd	February 16-17, 2009	Singapore	・Presentation of the result of the study on the ISM benchmark from each country. ・Discussion on needs and issues of the common ISM benchmark. ・Discussion on WG's Vision and Goals.

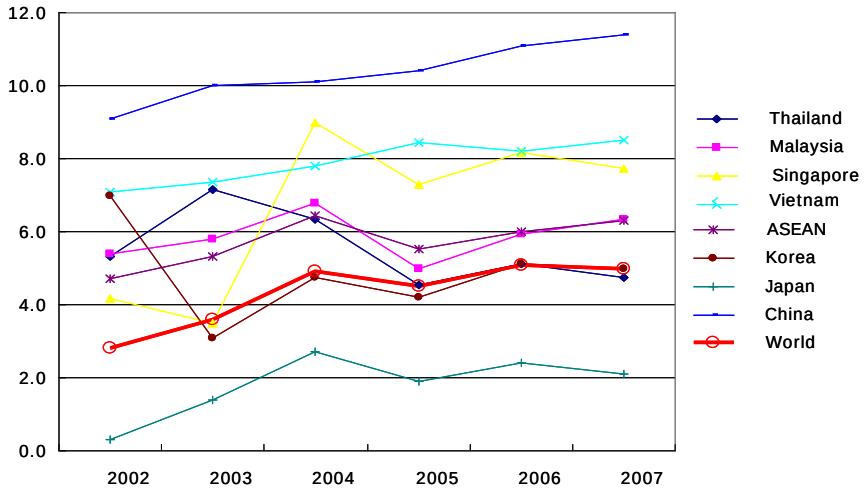
III. Research for Strengthening Information Security in the Business Sector

1. Economic Impact of Strengthening Information Security in Asia

1.1. Economy of Asian Countries and Current Status of Enterprise Management

(1) Economic Growth in Asia

Asia is growing rapidly in comparison with the world average. The real GDPs of the world grew by 2.5% to 5% annually from 2002 to 2005. Meanwhile, the member countries of the ASEAN and Asia, excluding Japan, achieved growth rates exceeding the average global growth rate (see Figure 1-1-1 Supported by the strong growth rates, these countries have assumed more important roles in the world economy.



Source: IMF, "World Economic Outlook 2008" and World Bank

Figure 1-1-1 Real GDP in Asia (Annual percent change)

The importance of these countries to world trade and the global economy has been increasing. For example, Asia's share of world trade is becoming larger. In particular, the share of world trade in the export of goods grew from 14.3% in 1980 to 26.6% in 2005.

The economic development in the region is sustained by an increase in direct investment in the region and expansion of Economic Partnership Agreements (EPA). As a qualitative shift, the economy in the region has been moving toward a knowledge-based economy with growth in the knowledge-intensive and high value-added industries.

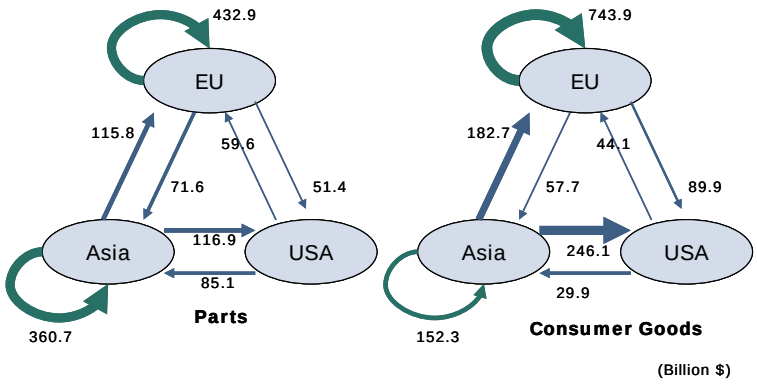
As the importance of the Asian region has been increasing, it has assumed a

more important role in establishing a system that supports the economy and trade. We can expect an initiative within the Asian region to establish such a system will promote Foreign Direct Investment (FDI) in the region and consequently lead to strengthened economic competitiveness.

(2) Progress of Global Value Chain in Asia

The value chain in the Asian region has expanded remarkably with the growth in the Asian economy. Asia's evolving production networks connect the labor, capital, and techniques of different countries in the region more effectively. The characteristics of the Asian region's value chain include the development of the division of labor. One of the Asian region's characteristics is that it has a structure to actively trade intermediate goods within the region and export finished products to the rest of the world as a the "world's factory." The production and distribution networks of Asian countries can cover not only one country but also the whole Asian region.

As shown in Figure 1-1-2 (left), the amount of trade of parts of the Asian region has been increasing close to that of the EU with its great regional economy. Meanwhile, Asia's ratio of exports of finished products within the region is much lower than that of the EU. As shown in Figure 1-1-2 (right), more consumable goods are traded for export than for consumption within the region. This shows the image of Asia as the "world's factory" as well as the fact that the Asian economy cannot realize self-sufficient, stable growth within its own region as of now. However, the great popularity and diversity of Asia have great potential as the last consuming region.



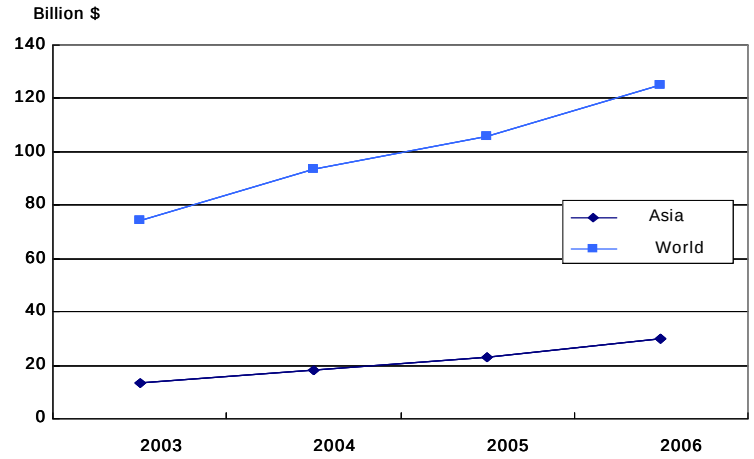
Source: IAA, Research Institute of Economy, Trade and Industry, "RIETI-TID 2007"

Figure 1-1-2 Trade in Consumption Goods Between Asia, U.S.A., and Europe (2006)

In the future, with additional progress in interregional trade and development of the trend toward a service economy in the Asian region, not only will companies more actively collaborate with one another but the quality of their collaboration will change. It is expected that higher-level information, such as design, financial, and personal information will be exchanged among companies in addition to order information in simple SCM.

(3) Development of Outsourcing and Offshoring

Outsourcing among companies and especially offshoring, which is cross-border outsourcing, have been developing in Asia (Figure 1-1-3). As no official statistics exist for the outsourcing/off-shoring market, we have no choice but to depend on estimates. For example, seeing the growth of exports in computer and information services, we can see that Asia's exports of computer and information services were $30 billion in 2006, representing an increase in the average rate of 26% from 2000. We can estimate that the exports of computer and information services include offshore IT outsourcing (ITO).

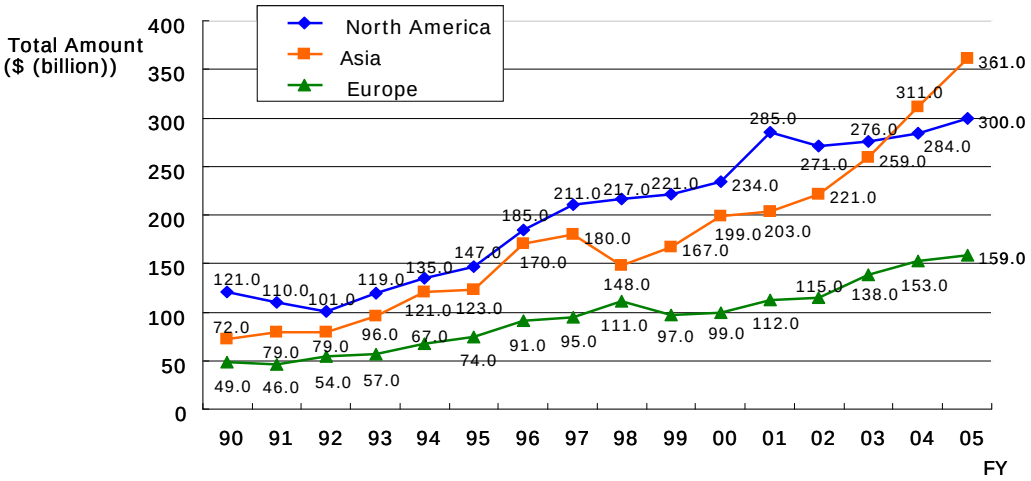


Source: WTO, "International Trade Statistics 2008"

Figure 1-1-3 World exports of computer and information services by region

Sales by foreign branches directly reflect the trend in enterprise offshore outsourcing. Generally, manufacturers outsource local partners through their foreign branches and subsidiaries instead of outsourcing foreign partners directly. Figure 1-1-4 shows the sales by foreign branches in manufacturers by region. As seen from the figure, the enterprise sales by foreign branches in

Asia grew at a higher rate than those of other regions. This shows how much outsourcing by manufacturers in the Asian region has developed.



Source: METI (Japan), “Manufacturing Products White Paper”

Figure 1-1-4 Total sales by foreign branches (manufacturing) by region

However, we have to keep in mind that outsourcing has both positive and negative sides. The positive sides include streamlining enterprise management and activating trade in the region, while the negative sides include causing serious damage to enterprise management and weakening enterprise competitiveness due to leaks of important information, such as enterprise expertise and intellectual property if it is implemented improperly.

(4) Evolution of Cooperate Management Through IT

Implementation of IT in companies has drastically changed ideas about enterprise management. IT enabled businesses to collect and analyze a diverse range of information on business operations more widely and quickly, which substantially improved the speed and accuracy of enterprise management. For example, only the production field could conventionally grasp information on factory inventory in real time. However, the whole company, including the headquarters and sales department, can grasp information using IT and reflect it in sales activities and production planning. With the development of group management and outsourcing, advanced companies have implemented IT and shared enterprise information beyond the borders of a single company (Figure 1-1-5).

Because of this, in addition to information security for conventional internal information management, the importance of information security measures for intercompany information management has been increasing.

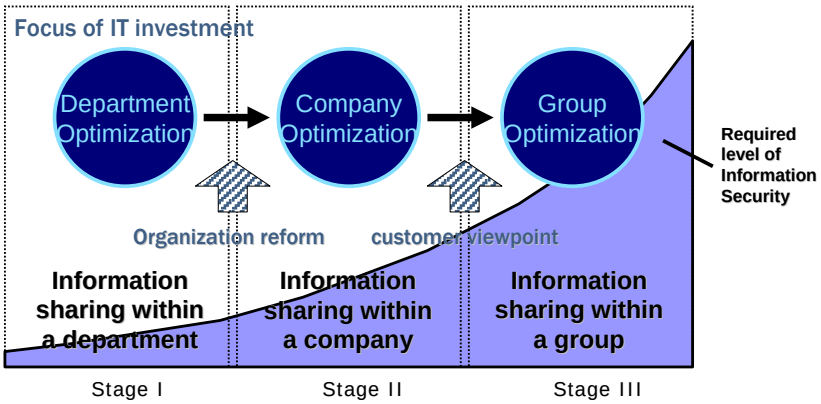


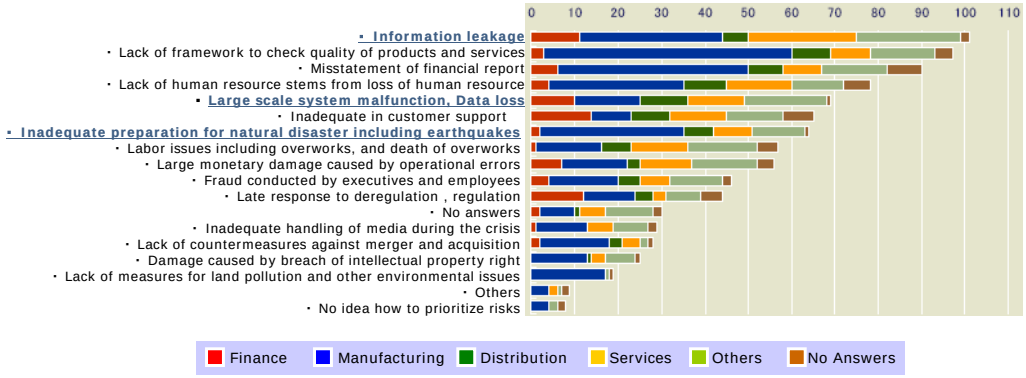
Figure 1-1-5 Progress of IT investment and enterprise management

As we have seen so far, development of outsourcing and progress of enterprise management require constructing a more advanced cross-border common infrastructure suitable for a knowledge-based economy and appropriate for the knowledge-based economy era. Ensuring enterprise information security plays a significant role as part of this effort.

1.2. Current Status and Challenges of Enterprise Information Security Measures

(1) IT Risk Management

IT risks have accounted for more enterprise risk management. Figure 1-2-1 shows the results of a survey of Japanese companies. The results show that information leakages, information system failures, and risks to business continuity are placed higher among the business risks companies must handle. These are risks targeted for information security management.



Source: Tohmatsu Enterprise Risk Research Institute, “Questionnaire Survey on Enterprise Risk Management 2007”

Figure 1-2-1 Business risks to be prioritized (By Sectors)

Management of IT risks, including information security risks, is an important issue for companies, and it has been pointed out that the important issue in enterprise management is the extent to which these risks should be addressed is unclear because the risks are difficult to evaluate quantitatively. Considering information security measures from the perspective of business entrepreneurs, they can hesitate to invest in information security that is not directly linked to their interests, in many cases, because they have no criteria to determine how to specifically handle these risks and how much they should invest in security.

The ISM benchmark[1] developed by the METI in Japan easily evaluates the risk levels that companies face and provides an indicator to determine whether taking information security measures by knowing a relative position from other competitors’ measure levels.

ISO/IEC 27001 and 27002, the international standards used from the perspective of information security management, provide models for information security management, but do not indicate any levels. There are, therefore, no tools to measure common information security levels to be used internationally at this time.

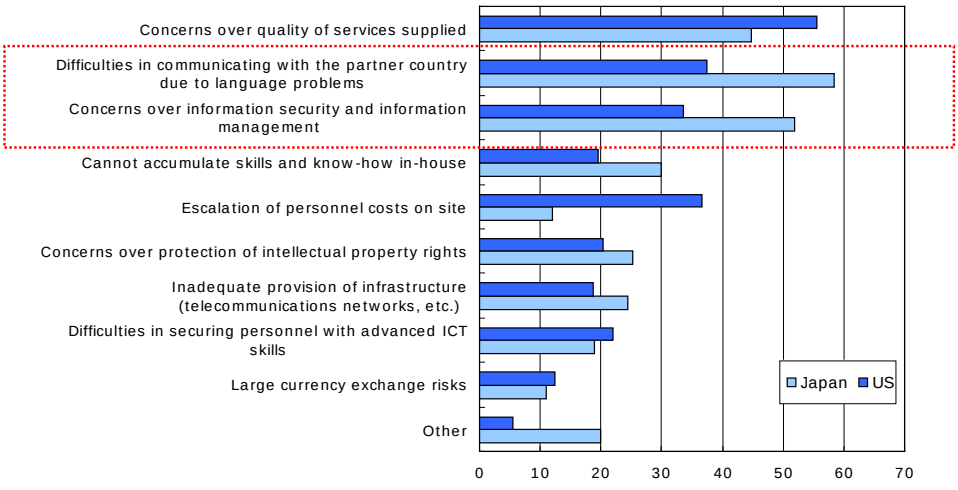
The ISM benchmark is intended for Japanese companies. However, this is effective as a draft in order to consider a tool (common ISM benchmark) to measure information security levels agreed upon internationally.

[1] For ISM benchmark, see Appendix 2.

(2) Risk Management in Outsourcing

The development of outsourcing consequently leads to an increase in the amount of information flowing among companies. In addition, companies that collaborate closely with one another through the supply chain increase their interdependency in one way. This requires companies to handle outsourcing risks, especially information security risks.

According to a survey of Japanese companies, ensuring information security is recognized as an important problem in performing offshore development in companies together with outsourcing quality and communication with partners (Figure 1-2-2). This can be expected to be a more important problem as services to be targeted for outsourcing are more sophisticated. It is striking that the respondents identified problems in communication with their business partners. When this is interpreted literally, it is a problem of language. However, when it is seen from the perspective of information security, it indicates there can be a risk communication problem. In this case, a system that assists risk communication between a company and an offshore outsourcer can solve these problems in implementing offshore outsourcing by a company.



Source: MIC (Ministry of Internal Affairs and Communications, Japan), "Study on development and influence of offshoring" (2007)

Figure 1-2-2 Challenges in advancing offshore development

(3) For establishing a strong value chain in Asia

In order to achieve continuous economic development in Asia, where growth has continued by leading in trade, trade must be expanded further in addition to expanding intraregional consumption. Because of this, it is important for companies in the Asian region to collaborate more closely and to promote foreign direct investment (FDI) in the region. With this, we can outpace the fierce competition by meeting market needs more flexibly and quickly and enabling the manufacture of optimal products in optimal areas.

In order to establish a stronger and more reliable value chain beyond the frameworks of countries and companies, risks involved in collaboration among companies must be managed. For this purpose, it is important for entities in the value chain to have a common understanding of risks involved in the collaboration among companies. In addition, communication measures against these risks are also important.

The following new measures against these risks are required for companies as we have seen so far:

- Measures against new risks involved in management innovation using IT
- Measures against new risks involved in using outsourcing

In addition, we saw that the role of information security management was critical in dealing with these risks. Therefore, the establishment of information security management in the value chain is a required element of risk management in the value chain (Figure 1-2-3).

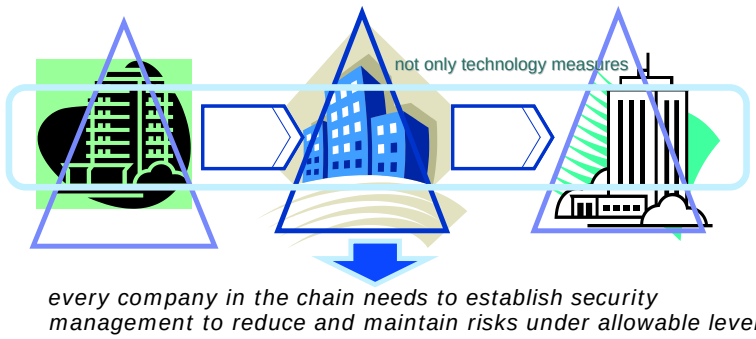


Figure 1-2-3 Importance of information security management in establishing the value chain

The common ISM benchmark can be one solution to the challenges facing information security management in the value chain. Conventionally,

companies shared no common method to easily evaluate their information security levels. However, the common ISM benchmark can provide such a method.

Of course, though the common ISM benchmark does not solve all of the challenges, it can be the first step toward establishing information security in the value chain. It is also important for the Asian region, which has become an important part of the world economy, to take the initiative in developing the common ISM benchmark from the viewpoint of establishing a new collaborative model in the Asian region.

2. Current Status of Information Security in Business Sector

In this chapter, we studied the requirements that the common ISM benchmark must meet in the future. First, we conducted a survey on the status of enterprise information security in each Asian country ((1) Current Status of Information Security in the Business Sector). This survey was conducted because it was estimated that different countries have different issues regarding enterprise information security and enterprise information security levels.

Second, we conducted a survey on national policies on information security especially intended for the public sector in Asian countries ((2) Government Policies Related to the Business Sector). This survey was conducted because it was estimated that regulations on information security, standards for compliance, and governmental role for information security measures could influence enterprise activities substantially.

Third, we conducted a survey on functional requirements for the common ISM benchmark by asking companies in countries all over the world to try the ISM benchmark developed by the METI and operated by IPA ((3) Study on Information Security Management Benchmark).

Last, based on the results of these surveys above, we studied the need for the common ISM benchmark ((4) Need for Common ISM Benchmark). Appendix 3 shows the questionnaires given to these companies in (3) and (4) just for reference.

In addition, because the ISM benchmark has already been frequently used in Japan and the need for it has been confirmed, we considered (3) and (4) based on past operations instead of trials.

2.1. Malaysia

(1) Current Status of Information Security in Business Sector in Malaysia

Information technology has moved Malaysia a step ahead to spur economic growth from a production-based economy (p-economy) to a knowledge-based economy (k-economy) when the former Prime Minister, Tun Dr. Mahathir Mohamed, launched the K-economy campaign in 1991. This gives convergence to appreciation of content creation where the digital economy based on information technology increases global opportunities and brings Malaysia into a more competitive market.

The business sectors in Malaysia face major challenges to addressing the dynamic nature of cyber security threats where ignoring information security

requirements may legally jeopardize business. In order to minimize the risk, various actions have been taken in the legislative area, such as reviewing and enhancing Malaysia's cyber laws, to ensure that the country is in line and complementary with international laws, treaties, and conventions. Proper studies were conducted with cooperation from the public and private sectors to better improve regulations since information exists in many forms and requires a proper method to protect the security of information. Malaysia has several acts pertaining to information security, which are the Communication and Multimedia Act 1998, the Computer Crimes Act 1997, and the Digital Computer Act 1997.

Corporate sectors in Malaysia are beginning to look into Information Security Governance and implementation within their organizations. Areas of focus are the protection of information assets against business risks and implementation of risk management because the data, information, and software had become invaluable assets of business as a whole. This is in line with the increasing value and quantity of data transmitted and stored on the systems. The Malaysian government encourages collaborative action by the public and private sectors at the local and international level. Seminars and knowledge sharing sessions are conducted to share and disseminate information on information security with the objectives of creating public awareness and further strengthening public-private cooperation in protecting the Critical National Information Infrastructure or CNII sectors. As the agency entrusted by the government to become a one-stop center for cyber security issues, CyberSecurity Malaysia has represented Malaysia at various IT security conferences and has earned the trust of other countries to lead IT security committees and collaborations. CyberSecurity Malaysia has been elected to chair the Asia Pacific - Computer Emergency Response Team (APCERT) for the term 2007 –2009. Recently, CyberSecurity Malaysia was elected the chair for the Organization of Islamic Conference - Computer Emergency Response Team (OIC-CERT) during the term 2009 until 2011. These appointments show the roles played by the country's local institutions in the international arena and how the efforts were accepted and recognized in the field of cyber security.

Information security awareness campaigns begin to impinge the business community when organizations begin to protect their information from being breached and the confidentiality, integrity, and availability of the information

are intact. The framework for information security was established whereby the protection of information could be achieved by identifying and implementing a suitable set of controls, and it could be managed systematically by implementing the Information Security Management System (ISMS). ISMS is part of the overall management system based on a business risk approach to establish, implement, operate, monitor, review, maintain, and improve information security. The business sectors in Malaysia have shown their intention on this critical matter when 26 local organizations were awarded the ISO/IEC 27001:2005, an accreditation for those who had demonstrated full compliance towards international standards for information security. The number of organizations adopting the ISMS and pursuing certification has been increasing each year, and this represents a positive indicator that the business sectors are beginning to realize that information security is a crucial and worthwhile investment.

In line with information security is the development of secure communications over the Internet. This is because critical information regarding Internet operation is stored in distributed databases. In conjunction with this, the .my domain registry, as the sole agency responsible for the registration of domains that end with .my in Malaysia, has introduced the Domain Name System Security Extension (DNSSEC). The system is designed to protect clients in the various sectors of government, education, and telecommunications from forged domain name server (DNS) data, pharming, phishing, and other malicious cache poisoning attacks. Using cryptographic technology, the information transmitted is protected.

Despite the many good things gained from the evolution of the technology in the cyber world, it has also created malicious threats and multiple challenges that need to be properly addressed, especially the information security issues. In the information technology era, the best formula or technology today does not ensure safety tomorrow. For this reason, continuous effort and cooperation from both the public and the private sectors must secure and protect the national interest. Awareness of information security is being applied to all levels of society to ensure stability, social well being, and the creation of wealth.

(2) Government Policies Related to the Business Sector

The growing dependency on information systems, coupled with the risks, benefits, and opportunities such dependency entails, has highlighted the need to properly address information security matters. Malaysia has developed the National Cyber Security Policy (NCSP) as a proactive step in protecting vital sectors in the country by identifying the critical national information infrastructure (CNII). Ten CNII sectors were identified as follows:

a. Government Services
b. Energy
c. Information and Communication
d. Defense and security
e. Food and agriculture
f. Banking and Finance
g. Health Services
h. Transportation
i. Water
j. Emergency Services

Some of these sectors are critically dependent on ICT while others increasingly rely on computers and computer network systems to deliver essential services to the country. Disruptions to the CNII will cascade well beyond the vicinity of the initial occurrence and can potentially cause regional and national disturbances. The technology changes at a fast pace requiring proactive information security initiatives from the government and the CNII entities.

Under the NCSP, CyberSecurity Malaysia was established as an agency under the Ministry of Science, Technology, and Innovation or MOSTI to be a one-stop coordination center for all national cyber security initiatives with the following goals:

a. Reduce the vulnerability of the ICT systems and networks.
b. Nurture a culture of cyber security among users and critical sectors.
c. Strengthen Malaysia’s self-reliance in terms of technology and human resources.

In formulating the policy, five key aspects had been identified as follows:

a. Legislation and Regulatory
b. Technology
c. Public and Private Cooperation
d. Institutions
e. International

The government of Malaysia has the vision of making the Malaysian CNII secure, resilient, and self-reliant and, when infused with a culture of security, will promote stability, social well being, and the creation of wealth. Based on this vision, the implementation of the NCSP was divided into policy thrust areas as follows:

a. Effective Governance

The intention is for Malaysia to have a national information security coordination center. This is done by establishing CyberSecurity Malaysia. At least two main committees have been identified to oversee the implementation of the NCSP. They are the National Cyber Security Advisory Committee and the National Cyber Security Coordination Committee. The members of these committees consist of representatives from different ministries and regulators that oversee the operation of the CNII.

b. Legislative and Regulatory Framework

The objective of this thrust is to ensure that there are eventually adequate provisions in Malaysian law to address cyber crimes and to establish progressive capacity building programs for national law enforcement agencies. A study is currently underway to identify issues and challenges faced in the cyber environment, assess gaps in the current legislative framework, and provide recommendations on the types of amendments to present laws.

c. Information Security Technology Framework

This thrust is to expand the national certification scheme for information security management and assurance. This is done by developing and reviewing national information security standards and the establishment of local product evaluation labs to evaluate information security products under

international standards, such as the Common Criteria, to provide certification for IT product security functions. Malaysia is now a consuming nation under the Common Criteria Recognition Agreement. In addition, the ISMS ISO/IEC 27001 is being proposed for adoption by the CNII of the country.

d. Culture of Security and Capacity Building

This looks at the human aspects of the policy to reduce the number of security incidents within the CNIIs through the effective management of information security by improving awareness and heightening skill levels. This will be achieved by developing, fostering, and maintaining a national culture of security, standardizing and coordinating cyber security awareness and education programmers across all elements of the CNIIs, and establishing an effective mechanism for dissemination of cyber security knowledge at the national level. Minimum requirements and qualifications for information security professionals will be identified. Meanwhile ongoing training and certification courses, such as the CISSP and PCIP programs will be continued.

e. Research and Development Towards Self-Reliance

The ultimate aim is to gain acceptance and utilization of locally developed and commercialized information security products by formalizing the coordination and prioritization of cyber security research and development activities, enlarging and strengthening the cyber security research community, and promoting the development and commercialization of intellectual properties, technologies, and innovations through focused research and development, thereby nurturing the growth of the local cyber security industry.

f. Compliance and Enforcement

Strengthening the information security enforcement role in all regulatory bodies in the ten critical sectors will be achieved by identifying appropriate and available information security standards as a baseline guide for compliancy enforcement across the CNII, standardizing of cyber security systems across all elements of the CNIIs, strengthening the monitoring and enforcement of standards, and developing a standard cyber security risk assessment framework. Furthermore, compliance audit exercises by CNII elements will also be regularly conducted.

g. Information Security Emergency Readiness

This is to build CNII resilience against cyber crime, cyber terrorism, information warfare, or accidental damage through tested and proven Business Continuity Management planning. Malaysia has developed the National Cyber Crisis Management Plan. The Plan will provide guidance on the coordination of cyber incident responses locally and internationally, the cyber incident response plan and early warnings, and the conduct of periodic cyber drills.

h. International Cooperation

The objective is to strengthen Malaysia's international branding by spearheading the CNII protection initiatives, strengthening relationships with foreign government agencies in the field of information security, and increasing Malaysia's partnerships and participation in key international information security events. Initiatives under this thrust includes spearheading the Organization of the Islamic Conference – Computer Emergency Response Team (OIC-CERT), as well as participation in key international platforms such as the Asia Pacific Computer Emergency Response Team (APCERT) since 2002 (Elected Chair since 2007 - 2009), Forum for Incident Response Security Team (FIRST) since May 2003, and the Security and Prosperity Steering Group (SPSG) under the APEC Telecommunication and Information Working Group (APECTEL).

Malaysia will continue to move towards the secure, resilient, and self-reliant CNII as explicitly stated in the NCSP vision statement. Successful implementation of the policy will provide a robust CNII that will be able to meet the challenges and opportunities of technological advancement and that will help to achieve the objectives of Malaysia's Vision 2020.

(3) Study on Information Security Management Benchmark

A survey was conducted using the information security management benchmark (ISM benchmark) developed by the Information-Technology Promotion Agency of Japan in January 2009. The objective was to gauge the usability of the application in Malaysia and to obtain feedback from local business entities on the benchmarking tool. It is important to state that the

results of the survey are based on the opinion of participating individuals about the level of information security in their organization. The survey received feedback from 13 participants. The demographic is as follows.

a. The benchmark application categorized an organization as large if it employed more than 300 people. Therefore, 7, or 54% of the participants, came from large organizations.
b. The organizations are also categorized according to IT security level requirements. This is determined by the application based on answers to the questions. The organizations are divided into low, medium, and high IT security level requirements. Of the total, 85% of the participants came from organizations that require high IT security levels and 15% requires low IT security level.

The ISM benchmark compared the results of the survey against the results of more than 16,000 companies in Japan. The analyses are as follows:

a. In comparing the information security level by the size of the organization, more than half (54%) of the participants are above average. Of the large organizations, 83% are above average compared to only 40% of the medium and small organizations.

Based on the results, the larger organizations have better information security measures and awareness. This is probably because these organizations have the resources to have a dedicated IT and information security team. In addition, large companies tend to have IT framework and guidelines that include some level of information security for employees and offices. These will also include the necessary training and awareness programs on information technology and security.

b. Analyzing the participants' organization by business sector, more than half (54%) are above average. Of the large organizations, 83% are above average within their respective business sectors compared to 40% of the small and medium organizations.

This is because the large organizations tend to have activities on

information security initiatives such as awareness programs, IT framework and guidelines, compliance to standards such as ISMS ISO/IEC 27001, and training for employees. In addition, most participants from large organizations are organizations within the CNII of Malaysia. Coupled with the government NCSP initiatives, the information security level and awareness is sufficiently high.

(4) Need for Common ISM Benchmark

On the survey of the ISM benchmark, the participants' opinions are as follows:

a. Eighty-three percent say that the ISM benchmark is an effective tool for assessing the organization in terms of information security. However, it will only provide a high-level assessment on the matter.
b. Fifty-seven percent of the participants are of the opinion that the ISM benchmark is effective in obtaining general guidelines on information security measures and for comparisons of the information security level within the respective industries. Forty-three percent of the participants use the application to identify the problem domain in information security.
c. Most of the participants (86%) are willing to use the ISM benchmark in their organizations and consider it an effective tool in gauging the information security level of the organization. However, some participants disagree, saying that their organizations have developed in-house applications for this purpose.
d. Eighty-six percent of the participants would like to use the ISM benchmark as a tool to check the organization's information security level while only 36% would like to use it to check the supplier's information security level and to report the organization's information security level to the client.

Presently, only 29% of the organizations have received requests from their business partners to comply with certain information security measures, such as ISMS ISO/IEC 27001, the Payment Card Industry Data Security Standards (PCI DSS), and the International Ship and Port Facility Security Code (ISPS). On the other hand, only 14% of the organizations have asked their partners to

comply with international standards or the ISMS ISO/IEC 27001.

The ISM benchmark was widely accepted by the participants' of the survey where 64% said that the application was easy to use. However, there were some suggestions to further improve the application, which was discussed in the working group meetings.

2.2. Singapore

The following sections summarize the findings of the ISM benchmark study on the Singapore industry, as well as feedback from Singapore's participants and respondents on the ISM benchmark. The report covers the following aspects as proposed by the ERIA project consultant and chair for the Singapore industry and perspective.

(1) Current Status of Information Security in Business Sector in Singapore

Few national level security standards have been published in Singapore. Security standards in Singapore were mostly developed to provide specific guidance in areas that do not have equivalent international standards or industry best practices. Most businesses adopt and follow their corporate policies and comply with local regulatory requirements. The Singapore government (Infocomm Development Authority, IDA) also plays a crucial role building infrastructure and initiating programs to encourage best practices to develop competence in information security regulations and standards.

Few information security-specific surveys have been conducted at the national or industry level in recent years. As such, there is no specific report available to enable a detailed study. Nevertheless, related work, though limited, has been found to provide the needed background to support the needs of this project. We review the results of three known/related surveys:

- Microsoft Security Intelligence Report (SIR) release 5 (Nov 2008)
- IDA's Annual Survey on Infocomm Usage in Business (2007)
- Mini-survey of an Information Security Risk Management (ISRM) research project (2006)

i) Microsoft Security Intelligence Report (SIR) Release 5

The Microsoft Security Intelligence Report (SIR) was first published in late 2005 based on a collection of malware/trojan scan results provided by the Microsoft Malicious Software Removal Tool (MSRT), Microsoft Windows Defender®, Microsoft OneCare, and Safety Live Antivirus products, as well as other external security data sources. In this study, we reviewed the latest release, i.e., Release 5, of the SIR.[2]

Overall, Microsoft's analysis showed that stolen equipment accounts for nearly twice as many incidents as intrusion. A number of incident reports reviewed for this analysis further established that intrusions or accidental exposure of information on the Web had been going on for quite a while before being detected. Improper disposal of business records also accounts for quite a few incidents. Malware, which was cited in the previous volume of this report as being responsible for a small percentage of incidents in previous periods, was not blamed for any incidents reported in 2H07 or 1H08.

Based on the locale setting of the operating systems, Microsoft's MSRT provides a count of computers per million (CCM) to determine the location of computers checked by MSRT. Using CCM as a standard metric, Singapore's CCM increased by 52.2% in 1H08, from 5.0 to 7.6 (from 2H07 to 1H08). Relative to Japan (CCM 1.5 to 1.8), Singapore's malware status is comparatively higher, but closer to other neighboring economies, such as Malaysia (CCM 4.6 to 6.3), Hong Kong SAR (CCM 6.1 to 7.0), China (CCM 4.7 to 6.6), India (CCM 5.5 to 6.2), Australia (CCM 4.9 to 6.9), and New Zealand (CCM 3.8 to 6.0), sharing also the similar upward trend in 2008. These trends fair well compared to most of the Middle East (e.g. Saudi Arabia at CCM 22.2 to 22.3) and South America (e.g. Brazil at CCM 13.2 to 23.9) locations, showing that the risk of malware is being managed, though not as effective as in Japan.

[2] Source: Microsoft Security Intelligence Report v5 (http://www.microsoft.com/sir/) which was based on Open Security Foundation (OSF) Data Loss Database at http://datalossdb.org.

ii) IDA's Annual Survey on Infocomm Usage in Business (2007)

Conducted annually since 2002, the results of this survey are available online at http://www.ida.gov.sg/Publications/20061205092557.aspx#usage. Analyzing the report revealed that there are five subsections related to security and trust.

- Infocomm Security by Employment Size
- Confidence Level
- Security Education
- Barrier to use of Infocomm
- Barrier to use of Internet

Overall, most organizations adopt some form of information security solutions, with antivirus (57%), anti-spyware (45%), and firewall (44%) ranked as the top three technologies used, and the use of an intrusion detection system ranked the lowest (12%). Security education programs have also been used in 61% of organizations of more than 200 employees, but only 14% of smaller companies (10 employees or less) have a similar program. Lack of external suppliers and lack of resources ranked as the top two impediments to information security education.

While the 2007 survey revealed increased adoption of the Internet, whereby Internet use reached 67% (from 62%) and broadband growth to 52% (from 49%), about 11% of respondents remain either not confident or not confident at all in online transactions.

Keeping up with new software releases, lack of skilled personnel, and reluctant to learn new skills were cited as the top three impediments to Infocomm usage, respectively.

Security concerns, cost of development and maintenance of web presence, and cost of Internet connectivity were cited as the top three impediments to Internet adoption.

The survey results revealed the important role information security plays in an organization, affecting their perception of the Internet and Infocomm

technology, hence their efficiency and competitiveness, in which adoption is key.

iii) Mini-survey of an Information Security Risk Management (ISRM) research project (2006)

As part of an information security research project, an information security mini-survey was conducted in the 2005/2006 period to understand the extent of information security risk management issues and dilemmas in business and government organizations across the Asia Pacific region.

The mini-survey comprised 37 questions, which was used as a basis to guide a series of structured interviews with 30 respondents, to determine the similarity and differences of their security risk management challenges and their strategy and plans in managing those issues and dilemmas.

More than 50 requests for participation were sent to chief information security officers (CISO) and equivalent appointments in organizations in the Asia Pacific region. A total of 30 responses from respondents in Australia, China, Malaysia, Singapore, South Korea, Taipei, and Thailand were received. Several follow-up interviews were conducted following the responses with 12 participants to clarify their input and gather more information about their practices.

While the number of respondents (30) may not be considered statistically significant to represent all the industries and organizations involved in information security risk management, the results of the survey do provide a number of useful insights to the practices of the participating organizations. We share some of the key findings here for consideration:

1. The survey results highlighted that information security is now a recognized function in most enterprises, including government organizations, with significant senior management visibility, at a level that is not more than four degrees from the chief executive officer (CEO).
2. The prevalence of information security considerations was supported by 87% of respondents who reported having a security plan in their organizations, and 93% of the respondents base their plan on risk management decisions. However, risk decisions were

based on assessments made by different groups of stakeholders in the organization, including IT auditors (12%), business managers (14%), IT Project manager/team (19%), IT/operation risks (24%), and IT security staff (26%). External consultants (2%) appeared to play an insignificant role in risk assessments.

3. In terms of knowledge and expertise, both at the senior and staff levels, the results showed only slightly more than half of the security executives (53%) and line personnel (67%) were adequately trained for their respective roles, demonstrating a lack of investment in security and competencies, which were two of the main inhibitors.
4. Security awareness was however regarded as one of the top three priorities in the respondent's security plans (similar to findings from other surveys).
5. While the main driver for information security was for business continuity, regulatory compliance remained a strong motivator, and the plans and activities were mostly based on a strategy that was bias towards a defensive approach, which is compliance focused. Nevertheless, this (compliance orientation) was only reported as a major challenge by 13% of the respondents.
6. Even though most respondents espoused their strategy as defensive-oriented, security monitoring and disaster recovery were listed amongst the top three priorities in approximately one-third of the responses. However, the high emphasis on patch management (73%) and change management (67%) supported the view that their actual practice was for a responsive system of information security risk management.

(2) Government Policies Related to the Business Sector

i) Information Security Policy and Effects on Business

Existing laws (acts) requiring business compliance include both industry-specific, and non-industry specific. The Singapore Banking Act (1970) has mandated strong security measures for online banking and IT outsourcing, including mandatory two-factor authentication, provision for business continuity and ICT disaster recovery, and data protection in IT

outsourcing. Singapore is one of the first countries in the world to enact a law that addresses issues arising in the context of electronic contracts and digital signatures. The Electronic Transactions Bill was introduced in Parliament on 1 June 1998 and passed on 29 June 1998. The Act came into force on 10 July 1998. [3]

In terms of personal privacy protection, the government's position has been a vertical approach, enforcing such protection on specific sectors where such requirements are clear and protection therefore needed, for example, the financial sector, which is based on specific provisions in the Banking Act (Section 47 on banking secrecy). For other business industries, the government has been promoting a self-regulating approach with guidance provided by industry organizations.

Against the proliferation of computer and Internet related crimes, the government also enacted new laws, such as the Computer Misuse Act (1993), Electronic Transaction Act (1998), Copyright Act (1987), Spam Control Act (2007), Terrorism Act (2007), and amendments to existing laws, such as the Evidence Act (1893) to permit use of digital evidence, to address related requirements and challenges.

To build confidence and enable trust in online and electronic commerce and related transactions, besides the ETA, a National Trust Council (NTC) was formed in March 2001. NTC established the TrustSg trust mark scheme, which has since resulted in the formation of the Asia Pacific Trustmark Alliance to promote similar schemes regionally. To date, 257 online sites have the TrustSg marking. A Model Data Protection Code (10 principles)[4]

---

[3] The Singapore ETA follows closely the UNCITRAL Model Law on Electronic Commerce, which sets the framework for electronic laws in many countries. The Electronic Transaction Act (ETA) also includes the "Security Guidelines for Certification Authority", requiring compliance with the then BS7799-1/2 standards. The full text of the ETA can be found at the Singapore Statutes Online website. (http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?actno=REVED-88&doctitle=ELECTRONIC%20TRANSACTIONS%20ACT%0a&date=latest&method=part&sl=1)

[4] This Model Code outlines the minimum requirements for the protection of personal information in the form of electronic data ("personal data"). This will assist organizations in developing and implementing

and an E-Commerce Risk Management Framework[5] (for online merchants) have been developed to promote self-regulation in the area of personal privacy protection and information risk management for industries not governed directly under specific regulations.

ii) IT Security Standards

The development, adoption, and promotion of IT security standards are jointly undertaken by SPRING Singapore and IDA through the IT Standards Committee (ITSC). The principle approach to standardization has been to adopt available standards directly (without localization or local re-numbering) and supplemented by Singapore Standards (SS) for specific requirements and areas of concern.

The following areas have been given more focus from the standards development perspective, in view of their strategic positioning in Singapore's economy, and the occurrence of numerous disasters around the region in the recent years.

- SS 507 provides for the certification of ICT Disaster Recovery Services, targeting the providers. SS 507 guidance, which had also been standardized as ISO/IEC 24762 in 2008.
- SS 540 is a recent update to the Technical Report, TR 19, providing guidance and a basis for certification of business continuity management. SS 540 is applicable to business organizations.

In 2008, the Singapore government set aside $30 million to help local companies and suppliers of the national critical infrastructure (NCI) to implement the SS540 standard.

---

policies and procedures to be used when managing personal data. The Data Protection Code document is available online at http://www.trustsg.org.sg/downloads/Data_Protection_Code_v1.3.

[5] The E-Commerce Risk Management Framework is available online at http://www.trustsg.org.sg/downloads/RM_Framework.pdf.

iii) Singapore InfoComm Security Master Plan

In April 2008, the government also announced Master Plan 2.0 (MP2),[6] which includes a S$70 billion investment over a five-year period to engage both the public and private sectors even more deeply in securing Singapore's cyberspace. MP2 includes the following:

- Hardening of national infocomm infrastructure and services;
- Enhance infocomm security competence;
- Cultivate vibrant infocomm security ecosystem; and
- Increase international collaboration.

(3) Study on Information Security Management Benchmark

i) Approach and Process

As reflected in the discussion session held during the first workshop in Tokyo, and the subsequent e-mail exchanges, there is a gap in the understanding of members' role in the participation of this study project. In any case, efforts were made to approach individual contacts in Singapore to gain support for the conduct of the survey directly. Four individuals were approached, and each helped to further approach their contacts in Singapore to cover up to 10 companies. Four organizations (two security companies, one education institution, and one IT provider) agreed to participate. However, one participant was not able to pass question number seven and gave up after eight tries. The participant was finally able to do so subsequent to the workshop. Nevertheless, the PDF reports were not available on time for the workshop, and to date, only three of the four reports have been downloaded.

Reflection

There are several contributing factors on the less than ideal outcomes, which were also anticipated in the conclusion of the first workshop:

[6] More detailed write-up available at http://www.ida.gov.sg/News%20and%20Events/20080417090044.aspx?getPagetype=20.

- Timing – the major work period coincides with long holiday season – Christmas, New Year, and lunar New Year holidays.
- Insufficient resources for socializing and engaging contacts to gain full support and ensure adequate completion of the survey.
- Members of the ERIA Project are in fact not the best resources to use for conducting the survey.

ii) Analysis of Survey Results

This section analyzes the results of the 25 ISMS questions answered by the participants.

Table 2-2-1 Attributes of respondents

	Total	**Size**		**Type of Industry**
		Large	**SMB**	
Singapore	4	0%	100%	IT security companies, education institutions, IT product company

In the surveys, two of the four respondents are responsible for information security in the companies. One of the participants (responsible for information security) further seeks formal management approval prior to responding to the questions online.

One of the four survey PDF reports has not been made available for this report. The following analysis, including those in the next section, is therefore based on the findings from the three reports that are available.

The small number of respondents does not provide for practical statistical analysis. Nevertheless, all three organizations are assessed as Group 1 organizations processing high risk and/or critical information. The results further showed that all organizations have some form of above average information security practices in place, supporting other survey (such as the IDA survey) findings discussed in the earlier sections.

Table 2-2-2 Summary of ISM benchmark assessments including comparison results

Participant	**Orgn**	**T-Score**	**Group 1**		**Large Organization**		**Same Industry**	
			Ideal (125)	**Ave (5)**	**Ideal (125)**	**Ave (5)**	**Ideal (125)**	**Ave (5)**

A Total Score	97	58.7	100	79	102	84	100	76
A Average Score	3.9		4.0	3.2	4.1	3.4	4.0	3.0
B Total Score	69	44.9	100	79	102	84	100	83
B Average Score	2.8		4.0	3.2	4.1	3.4	4.0	3.3
C Total Score	76	48.4	100	79	97	74	100	83
C Average Score	3.0		4.0	3.2	3.9	3.0	4.0	3.3

Both participants B and C were from IT security organizations, and their average score worked out to be the same (average of 3.3 points) compared with the same industry type, even though their individual overall and T-score differed. Given the small samples involved, it was not possible to draw any conclusions from this observation, even though it seemed to indicate that differences in practices (as captured by the overall and T-Score) appeared to have low impact when compared with the same industry type, which therefore may challenge the usefulness of the benchmark itself—since the benchmark is meant for comparison with the same industry.

On the other hand, while organization A had a high overall score (97) and T-Score (58.7), it had a lower average (76) when compared to the same industry type (lower than participants B and C's scores in that column). There is insufficient data to draw a conclusion on whether different industry types have a different emphasis that results in the differences, or there is no direct correlation between the organization's overall score/T-score and the metrics with which the industry is being compared. If this is true, then it would also raise questions on the usefulness of the benchmark results.

(4) Need for Common ISM Benchmark

This section analyzes the results of the additional six questions on the ISM benchmark.

- Needs toward a common ISM benchmark
- Expected function of common ISM benchmark
- Roles of common ISM benchmark
- Issues

i) Need for a common ISM benchmark

Based on the results of Q1 and Q2, we analyzed the needs for a common ISM benchmark. The findings and comments received are tabulated in the following tables (2-2-3 and 2-2-4), which are self-explanatory.

Two out of the three respondents are in favor of the ISM benchmark, finding it an effective tool, and willing to adopt it for their benchmarking purposes.

Table 2-2-3 Q1-Is the ISM benchmark effective in assessing your company's information security level?

	Yes	**No**	**Comment**
Singapore	2	1	Yes: - Fairly comprehensive; it is able to provide an answer to the question asked; - All of the above provided answer. No: - Current approach appeared to be at a level that was too high, which essentially only answered the question as to whether an ISM was in place. - Unlikely to see significant changes in the survey results once ISM has been implemented. - Lack of ISM itself cannot be the justification for implementing the ISM benchmark.

Table 2-2-4 Q2-Are you willing to use the ISM benchmark in your company?

	Yes	**No**	**Reason (Comments)**
Singapore	2	1	Yes: - It needs improvements in reducing repetitive questions, easier to understand questions in terms of its grammar and construction and the way it is structured. - To check your company's information security level No: - Concern over misuse and breaches of survey data, require higher management approval and support.

Evaluating all the comments (both positive and negative), we can conclude that the benefits of an international common ISM benchmark are clear (to the participants involved). The need, however, may need to be assessed in conjunction with other business priorities relating to the implementation of information security, in particular, in today's economic situation.

It appears from interviewing the four contacts and their discussion with their individual contacts that the value of a benchmark is not deemed significant, especially when they need to provide information security status related data, for which they have concerns about protection as well.

There is also a concern that the data collected are being hosted by an authority specific to Japan rather than a regional or international organization.

ii) Expected function of common ISM benchmark

Based on the results of Q3 and Q4, we analyzed the expected functions for the common ISM benchmark. As depicted in Tables 2-2-5 and 2-2-6, participants are mostly in favor of the usability of the ISM benchmark and do not have any specific request for additional functionality. However, participants have expressed concern over the reliability of the tool, as well as the consistency and clarity of the language used (as it was translated from the Japanese version.)

Table 2-2-5 Q3-Is the ISM benchmark easy to use?

	Yes	**No**	**Reason (Comments)**
Singapore	2	1	Yes: - No reason given. No: - English construction and the way the links are constructed are confusing sometimes. - Structure of the survey could be improved - overlap and clarity of questions - PDF output placement not obvious

Table 2-2-6 Q4-Do you have any ideas about additional functions or the improvements for the ISM benchmark?

	Yes	**No**	**Reason (Comments)**
Singapore	1	2	Yes: - I think there is a bug in the software in that it refuses to allow submission when I answered the question and keeps asking me to repeat certain questions - Has the online system been tested as compatible with major browser software, and does it have specific setting requirements? No: - For the questionnaire: There are a number of overlapping questions; the structure of the survey could be improved. - For results output: Placement of PDF output function not obvious.

There seems to be some errors in the system that prevents completion of the survey by some individuals. The challenge was that the error message was not explicit in helping resolve the problem.

iii) Roles of Common ISM Benchmark

Based on the results of Q5 and Q6, we studied the roles and the significance of the common ISM benchmark with regard to the expansion of direct investment and outsourcing in Asia.

Table 2-2-7 depicts the requirements for compliance with specific security standards, both by the participants' organizations and their business partners.

Table 2-2-7 Information security measures requested by/of business partners

	Requested by business partners		**Requested of business partners**	
	Yes	No	Yes	No
Singapore	2	1	1	2

The following standards have been cited by the participants that

commonly required compliance: ISO 27001/2, ISO 9001, PCI-DSS, SAS-70, SoX, and company-specific requirements.

iv) Issues

This section highlights the issues that have surfaced through the study and evaluates possible options for realizing the common ISM benchmark.

With regard to the current ISM benchmark questionnaires, the following issues have been identified:

1. The questions are generic and do not provide sufficient information to differentiate the security strength of companies involved. As noted in Section 3.2, while the overall score and T-score for each participant differs, the differences found in the comparison with others in the same industry and same group did not differ (for two of the participants). This raises question on the usability of the current ISM benchmark, which at this point could not be confirmed due to the insufficient sample size involved.
2. The differences between scoring 2.x and 3.x are not significant to indicate what needs to be done to achieve progress.
3. Few SME and local companies would achieve more than 4 and even less will achieve 5. In fact, no participant in the study has achieved a 5-point rating (including other countries that participated).

On the needs for a common ISM benchmark for the region, evaluating the study and its results and comments received, the following have been identified:

1. Organizations are more focused on a specific certification scheme, such as ISO/IEC 27001 or SAS 70, which relates closely to compliance of local regulation or partners, client requirements, and standards. Such return on investment (or cost expenditure) is more justifiable than performing to a specific benchmark.

2. Actual business motivation for complying with a specific benchmark is currently non-existent.
3. There is also an obvious uncertainty or a lack of trust in the benchmark system and its provider, including the data store being held in a specific location.

To promote the adoption of a common ISM benchmark scheme, there is a need to include the various stakeholders in each location in the region, including relevant government entities, industry associations, or influential leaders in its development and endorsement. Ideally, a regional, non-profit, independent organization should take the lead for such an initiative and front the marketing, awareness, and implementation activities involved, but not an organization or individuals representing any government. Such a regional, independent organization may also host the survey data or establish and enforce legally binding agreements between itself and its members to ensure proper sharing, use, and protection of the survey data collected through the benchmarking system.

2.3. Thailand

(1) Current Status of Information Security in Business Sector in Thailand

The National Statistical Office first started working on a survey of overall Thai e-commerce in 2007. The objective is to understand the status of business sectors that provide online services (e-commerce). This includes business type, number of employees, product delivery, and payments. The survey collected data from May to June 2008 by using interviews and questionnaires. A total of 42,000 respondents from business sectors were involved in the interview and questionnaires, and only answers from 1,678 respondents are valid. The results are presented below.

i) Business general information

The majority of Thai e-commerce transactions (74%) are made by small-size businesses that employ no more than 5 employees. Of the respondents, 72.5% are B2C-type businesses.

Of the respondents, 29.4% are in the fashion and jewelry business, whereas 21.1% of the respondents are in the computer industry, electronic

device business, and internet-related business.

The majority of Thai businesses (33.7%) have used electronic transactions for three to five years. Almost 50% of Thai e-commerce businesses have both online and physical shops.

Seventy-five percent of total business profits from e-commerce are from markets within the country while only 24.7% are from oversea customers from the USA, UK, Japan, Singapore, Germany, and other countries.

ii) Business Transaction

A total of 42.2% of Thai e-commerce businesses support the use of online advertisements. The most favorite methods include an advertisement on web boards (66.7%), search engines (46.5%), and e-mail (42.2%).

There is an improvement in the trust in e-commerce. A total of 37% of e-commerce businesses initiate a privacy policy/statement. About 13.3% and 6.9% employ TRUSTe and BBB online, respectively. In relation to the use of a security policy, 31.6% adopt encryption technology, and 29.2% have watermark technology. Only 12.0% accept the use of digital certificates. A total of 31.2% have a security policy.

In relation to payment methods, 42.1% of the respondents provide both online and offline payment methods. Only 9.8% offer only in the online method, especially paying through e-Banking/ATM (59.2%), a middleman service (Paysbuy and Thai e-pay) (47.3%), and credit card (39%).

Most Thai business sectors use a variety of delivery methods such as by post (59.3%), messenger (46.3%), and courier (30.4%).

Concerns about *information security* and other IT issues include information security and virus concerns (21.3%), lack of confidence in e-commerce (20.7%), and ineffective ICT resulting in slow internet speeds (20.7%).

Finally, most Thai business sectors need assistance from the government. The assistance includes consulting and training (30.1%), advertising e-commerce campaigns (21.4%), and logistics management (19.6%).

iii) Conclusions

The conclusion is that e-commerce in Thailand is in the beginning stage, though most Thai business sectors are ready and willing to adopt

e-commerce into their business. In terms of information security, Thai business sectors seem to overlook information security, since a very small percentage of them have security concerns and a security policy. It is therefore highly recommended that the government build information security awareness.

Source: National Statistical Office, "Report of the Survey on Thai E-commerce Status in 2007"

(2) Government Policies Related to the Business Sector

The government depends on its personnel and assets to deliver services that ensure the health, safety, security, and economic well-being of the Thai people. In terms of technology, information systems must be secured against rapidly evolving threats that have the potential to impact confidentiality, integrity, availability, intended use, and value. To defend against these threats, an IT security strategy is required that accommodates changes in threat conditions, which may be sudden, and supports the continuous delivery of services. This dictates that the government tends to apply baseline security controls, continuously monitor service delivery levels, track and analyze threats to business sectors' IT systems, and establish effective incident response and IT continuity mechanisms.

The government must ensure that the IT security policy is an integral part of each stage in the system development life cycle. Security requirements and related funding must be identified and included in the planning, requests for proposals, and tender documents for IT projects.

The information security policy was included into the ICT master plan 2009 to 2014. The security subcommittee under the e-commerce committee was formed to assume responsibility for technical and political support for the e-commerce committee. The security subcommittee involves representatives from several organizations and specialists in IT security from both the public sectors and private sectors. In order to raise information security awareness in the business sectors, the security subcommittee has so far initiated the following:

- Promotion of information security governance and some related topics initiated by NECTEC (under the Ministry of Science and Technology) and the Ministry of Information and Communication Technology (MICT).

- Free seminar held by ISP club, ISA, Itsec, and other related organizations.
- ICT Master Plan and IT Security Policy Conference established by MICT

By conforming to the information security policy's operational and technical standards, a security team would be better prepared to prevent, detect, react to, and recover from incidents. ThaiCERT was established in 2000 under the National Electronics and Computer Technology Center (NECTEC) to handle computer crime, coordinate with related organizations, conduct studies on security standards, and actively develop the Thai version of security standards.

Source:

1. Treasury Board of Canada Secretariat: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12322&section=text#sec10.12,
2. Survey Sheet on Information Security in Asia (Thailand) by Komain Pibulyarojana and Chalee Vorakulpipat

(3) Study on Information Security Management Benchmark

We are conducting a survey on the ISM benchmark to explore the overall information security practices in Thailand. A survey questionnaire has been distributed to a selected number of different private sectors. The organizations (respondents) were selected randomly from SME to large companies. They were contacted by telephone or e-mail before sending the questionnaire.

A cover letter and attached questionnaire were sent by e-mail or post. They were asked to assess the security level by themselves, complete the questionnaire, and then return the assessment results and completed questionnaire by e-mail or post. Clear explanations of how to assess IT security and complete the questionnaire were also included in the cover letter. If the respondents had any queries regarding the ISM benchmark, they were welcome to contact us anytime by e-mail or telephone. It is very important to note that the organization name must be undisclosed and must not be reported in any publications or elsewhere. We have already informed the respondents of this policy.

An ISM benchmark assessment form was sent to a number of business sectors in January 2009. These include hospitals, banks, IT auditors, IT

solution businesses, and Internet providers.

So far, eight organizations returned the completed forms. Scores generated from the ISM benchmark for organizations A, B, C, D, E, F, G, and H are presented below. The results are summarized in Table 2-3-1.

Table 2-3-1 Organization scores

Topics	A	B	C	D	E	F	G	H
Security Policy	4	5	4	2	2	2	2	4
Business Continuity	1	4	4	2	2	2	2	3
Security Incidents	2	4	4	2	2	5	2	3
IT Systems Failure	1	3	4	3	2	5	2	3
Software Management	2	4	5	3	4	5	1	3
Security in Development	1	2	4	2	2	4	1	4
Network Access Control	1	2	5	2	1	3	3	4
Access Control-Application	1	5	5	3	2	1	3	5
Access Control-Data	1	5	5	3	2	5	3	5
Prevent Theft or Loss	1	5	5	2	2	3	3	5
ICT Network	1	2	4	2	1	4	2	4
Vulnerability	1	4	5	3	2	2	2	3
Malware	1	4	5	3	2	2	3	3
IT System Operation	3	4	5	3	2	4	3	5
Operational Environment	1	4	5	3	2	4	3	4
Document & Storage Media	2	4	5	2	2	4	2	4
Safe Installation	1	2	3	2	2	1	1	2
Third Party Access	2	4	4	3	2	2	3	3
Physical Security	2	4	4	3	3	1	3	3
Security Training	4	5	5	2	2	1	3	5
Employee Contracts	2	4	5	3	1	4	2	2
Outsourcing Contracts	2	2	3	3	1	2	2	3
Information Handling	3	5	4	3	2	4	4	5
Information Categorization	2	4	3	2	2	5	4	3
Security Organization	1	4	4	3	2	1	4	4

A few companies returned the completed forms. The interesting results depicted below are assessed in three selected business sectors (two are

regarded as large organizations and the other is a small to medium-sized organization). The organization background is presented in Table 2-3-2

	Organization A	Organization B	Organization C
Size	Big size (>300)	Big size (>300)	Small and Medium size (<300)
Group classified	Group 1 (high IT security level measures are required)	Group 1 (high IT security level measures are required)	Group 1 (high IT security level measures are required)
Organization type	Internet provider	Healthcare	Agriculture organization

Table 2-3-2 Organization background

Scores generated from the ISM benchmark for organizations A, B, and C are presented below.

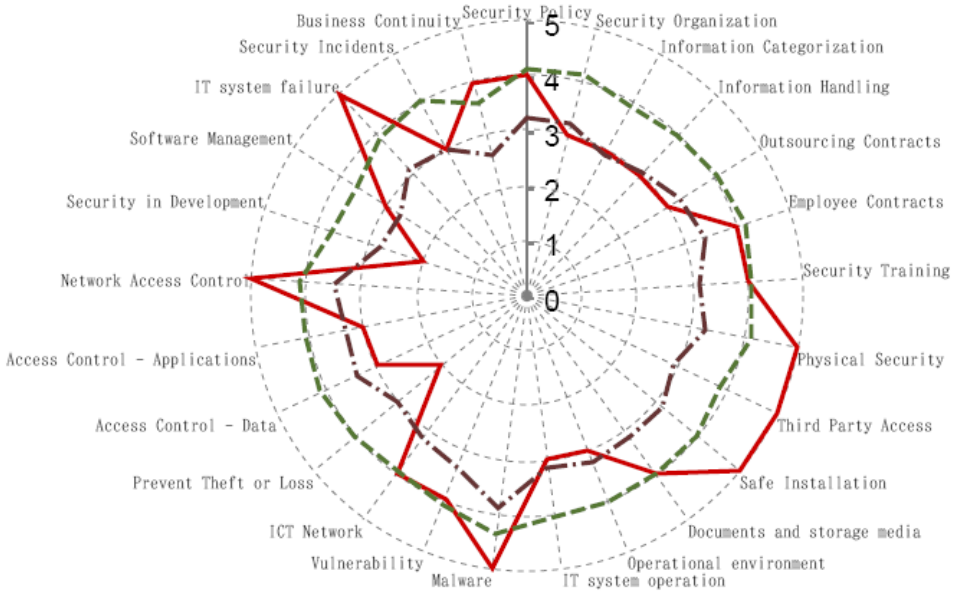


Figure 2-3-1 Scores for Organization A

Figure 2-3-2 Scores for Organization B

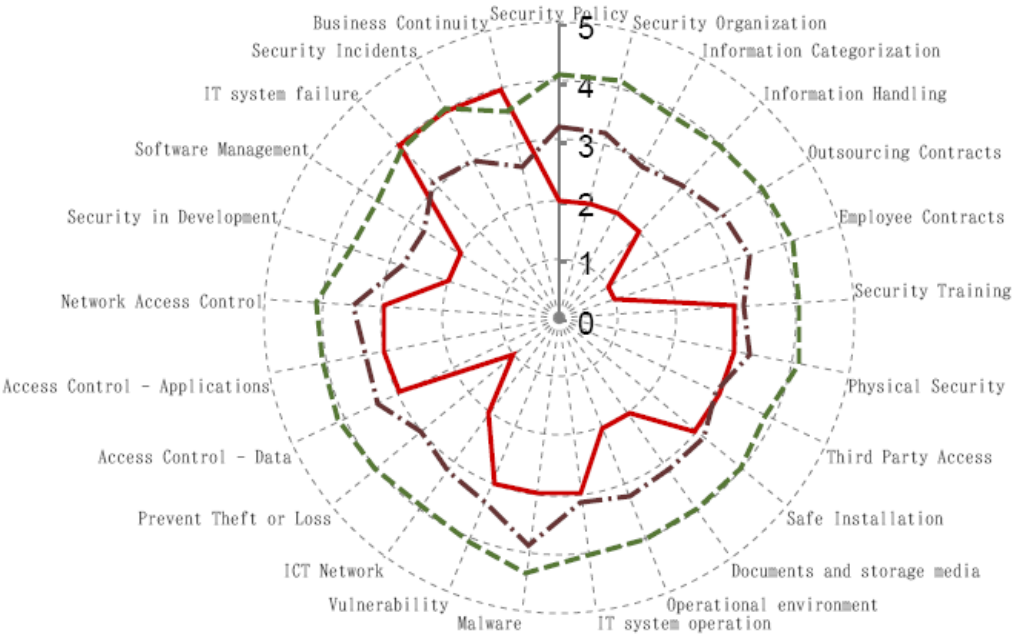


Figure 2-3-3 Scores for Organization C

The results are summarized in Table 2.3.3

Table 2-3-3 The summarized results (H= reach ideal security level; M= higher than or equal to average but lower than ideal security level; L= lower than average)

Topics	Organization A	Organization B	Organization C
Security Policy	H	L	L
Business Continuity	H	L	H
Security Incidents	M	L	H
IT Systems Failure	H	L	H
Software Management	M	L	L
Security in Development	L	L	L
Network Access Control	H	L	L
Access Control-Application	L	L	L
Access Control-Data	L	L	L
Prevent Theft or Loss	L	L	L
ICT Network	H	L	L
Vulnerability	M	L	L
Malware	H	L	L
IT System Operation	L	L	L
Operational Environment	L	L	L
Document & Storage Media	M	L	L
Safe Installation	H	L	L
Third Party Access	H	L	M
Physical Security	H	L	L
Security Training	M	L	L
Employee Contracts	M	L	L
Outsourcing Contracts	L	H	L
Information Handling	L	L	L
Information Categorization	M	L	L
Security Organization	L	L	L

Overall, the results show that Thai business sectors seem to overlook information security and lack skills and knowledge. Although some (such as

organization A) may show positive results, they still need to build awareness of some issues (such as access control, outsourcing contracts, and information handling). On the other hand, others have to improve employees' skills on almost all information security topics. Therefore, a call has been made to adopt the ISM benchmark to assess the level of information security within Thai business sectors.

(4) Need for Common ISM Benchmark

The ISM benchmark is a web-based self-assessment tool to visually determine the level of implementation of a company's security measures by responding to questions about the company profile and 25 questions on security. The ISM benchmark can be used to develop information security measure and in the operation phases to improve information security. In addition, the ISM benchmark conforms to international standards ISO/IEC 27001:2005.

In addition to the results in (3), all respondents found the ISM benchmark very useful and effective in assessing their organization's IT security level. This is because the ISM benchmark helps in the following:

- Understand the problem domain with regard to information security
- Acquire advice on information security measures
- Compare the information security level to the average.

Moreover, some respondents are willing to use the ISM benchmark in their organization to check the company's information security level. Some are not willing. This may be because of the following perceptions:

- The security issue is not important to their organization.
- The possibility of problems caused by lack of IT security is low
- Employees do not have sufficient IT skills.

Some of them commented that the ISM benchmark was not easy to assess and was time consuming.

In conclusion, from the results (3) and comments (4), business sectors have confirmed the need for the ISM benchmark. They strongly believe that this

self-assessment tool helps indicate their level of information security and will help to build information security awareness.

2.4. Vietnam

(1) Current Status of Information Security in Business Sector in Vietnam

The process of economic reform in Vietnam during the last few years has directly impacted and resulted in created a business sector in Vietnam. It has promoted the comprehensive development and diversification of trade, form of organizations and business areas. In recent years, Vietnam's enterprises are developing very rapidly in all economic areas, such as private enterprise, corporate enterprise, joint-stock companies, limited liability companies, foreign-owned companies, and joint ventures. From 2000 to the present, there have been more than 150,000 new enterprises established, accounting for 27% of the total country's investments (source: http://www.mpi.gov.vn).

Small and medium enterprises (SME) have contributed significantly to the economic development of the country and resolved many social problems such as jobs to reduce the unemployment rate and a better economic structure. Currently, Vietnam has more than 266,000 enterprises, exclusive of the nearly 3 million private business householders. SMEs reach 97% of the total country's enterprises, contribute 26% of the total national production, 31% of total industrial output production, 78% of total retail revenues, and 60% of national GDP (source: http://www.mpi.gov.vn).

Information and communication technology (ICT) has become the engine driving economic growth and the development of the business sector. The number of Internet users is increasing at the rate of 1% per year for narrowband and 2% per year for broadband. Currently, the rate of Internet users is about 35% of the population. The density of Internet use is 8 to12 subscribers/100 inhabitants with 30% of broadband Internet subscribers using ADSL. At the end of 2008, there were an estimated 2,048,953 broadband Internet subscribers and 20,834,401 Internet users (source: http://www.mic.gov.vn).

According to a study by the VDC[7], the demand for ICT use by enterprises is characterized by the following applications: e-mail (88%), information

[7] Vietnam Data Communication (VDC), http://www.vdc.com.vn

searches (64%), download/upload files (48%), extranet VPN (42%), e-commerce and e-business (24%), VoIP (12%), chat and information exchanges (4%), video conferencing (6%) and forums (2%).

Currently, 82% of enterprises have local area networks (LAN), 97% have Internet connections (mainly using ADSL), one-third of enterprises use e-commerce at 15% and 40% have their own websites. More than 90% of enterprises believe in the positive effect of the Internet. Only 3.6% of enterprises are unsatisfied about the benefits of the Internet.

A vast majority of companies use the flexibility and cost-effectiveness of the Internet to extend their networks to branch offices, customers and business partners. Information security (IS) has become critical to business performance, especially for companies depending on these networks for communication, transactions, and data sharing. Beside, the outsourcing investment has increased the concern for protection of sensitive information. Given the growing popularity of the Internet and networking transactions, including e-commerce, IS should not be overlooked.

Regarding the number of incident reports to VNCERT[8] from 2006-2008, the number of DNS attacks, spam, and e-mail phishing and fraud attempts has increased (Table 2-4-1).

Table 2-4-1 Number of incident reports to VNCERT during 2006 - 2008

	DDoS	Malware	Deface website	E-mail Phishing/ Fraud	DNS attack	Distr. Spam	Other	Total
2008	5	6	3	39	2	12	12	79
2007	5	9	13	12	2	-	6	47
2006	5	11	7	2			4	29

Most of the attacks in 2008 were e-mail phishing and fraud attempts (3 times more than in 2007). This was followed by new DNS attacks detected in 2007, which became more serious in 2008. Other attacks involved viruses, web hacking, DoS, and DDoS. Spam distribution is the new significant problem in 2008.

It is worthy to note that the number of virus attacks increases exponentially.

[8] Vietnam Emergency Response Teams (VNCERT), http://www/vncert.gov.vn

According to statistics by BKIS,[9] there were 33,646,000 computer virus attacks in 2007. The number of new viruses totals 6,752, thus the rate of virus attacks equals 18.48 per day. The number of virus reports to BKIS rose from 84 in 2006 to 563 in 2007 and to 2,375 in 2008. The percentage of PCs attacked by a virus in the business sectors is very critical: financing and banking (94%), services (97%), trade and commerce (99%), health services (90%), education (94%), and other sectors (94%). Figure 2-4-1 presents the total number of foreign attacks on Vietnamese websites in the period 2002 to 2008 according to statistics from Zone-H (http://www.zone-h.org).

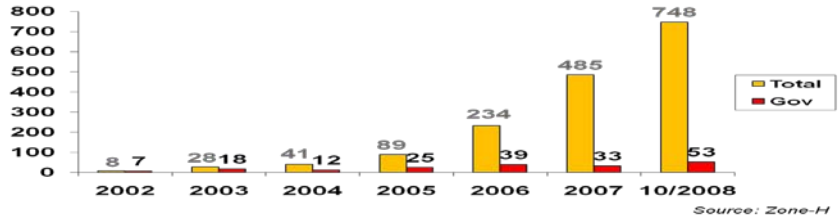


Figure 2-4-1 Number of foreign attacks to Vietnamese websites

In order to better understand the level of security awareness and the status of IS implementation in Vietnam, VNCERT and the Vietnam Information Security Association (VNISA) conducted a survey on information security from August to November 2008. A total of 2000 questionnaire sheets were sent to enterprises throughout the country and 400 sheets were returned. Of the 400 respondents, 40.2% were from government organizations, 24.8% from private companies, 14.4% from state-owned companies, 10.6% from foreign invested companies, and 9.9% from other organizations (Figure 2-4-2).

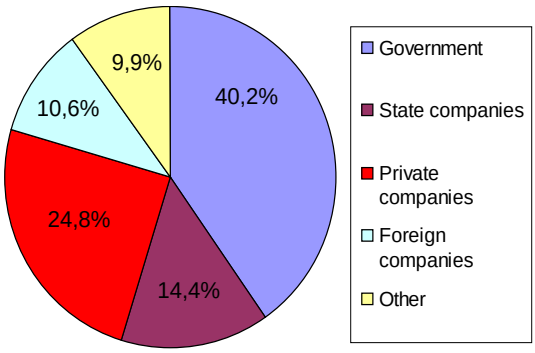


Figure 2-4-2 Classification of organizations

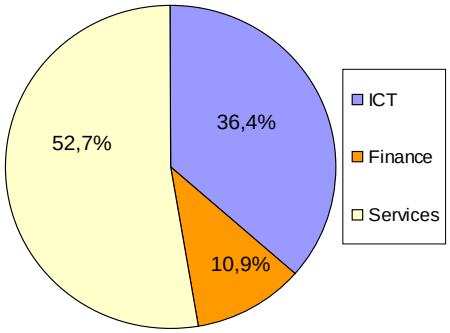


Figure 2-4-3 Classification of industries

[9] Bach Khoa Information Security Center (BKIS), http://www.bkis.com.vn

The respondents represented three major industry branches, namely services (52.7%), ICT (36.4%), and finance (10.9%) (Figure 2-4-3).

The survey findings reflected the fact that many enterprises still have not implemented sufficient countermeasures in preventing or tackling attacks. Many companies did not invest enough in incidents response procedures and security policies. Among the respondents, only 23.33% had adopted procedures for IS incident processing, 43.67% did not have any procedures, and 18.33% answered “not clear” (Figure 2-4-4). Similarly, only 29.33% had implemented a security policy, 32.67% wanted to have one soon, 20.33% did not know about a security policy (Figure 2-4-5).

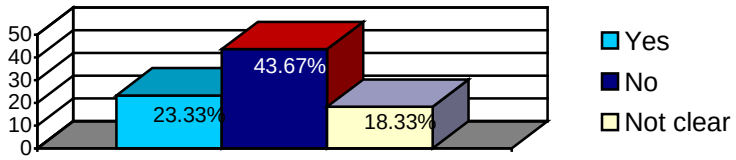


Figure 2-4-4 Percentage of companies with procedures for IS incident processing

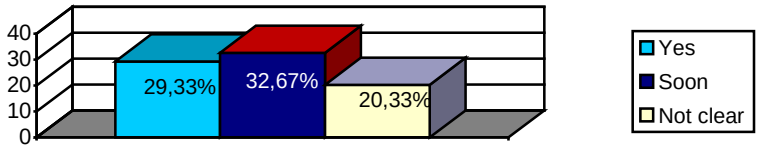


Figure 2-4-5 Percentage of companies with an information security policy

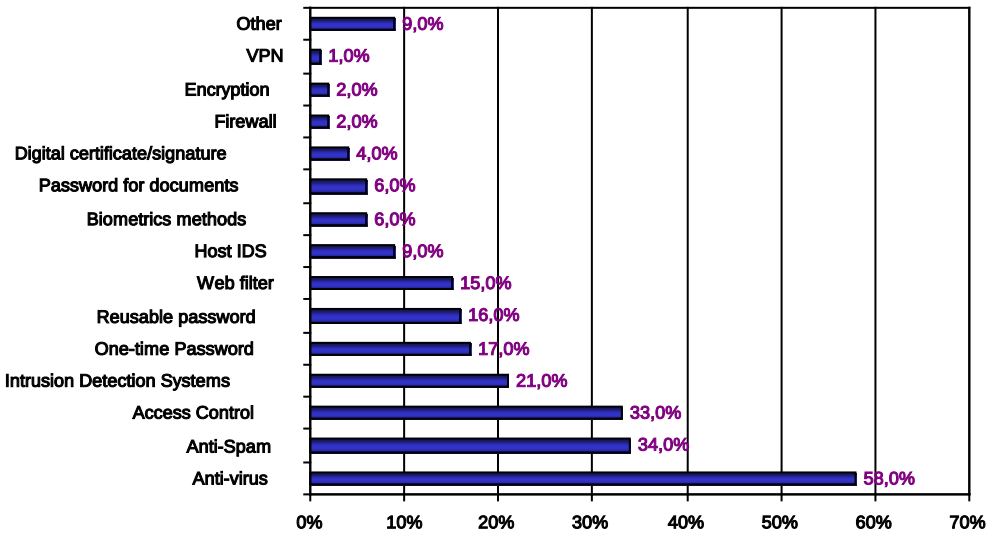


Figure 2-4-6 Survey of security technologies

One question included in the survey was to check which security technologies have been implemented for safeguarding company information. The three most popular security measures were antivirus software (58%), anti-spam (34%), access control (33%), one-time passwords (17%), and reusable passwords (16%) (Figure 2-4-6). Fifty-eight percent of enterprises used basic security tools like antivirus programs. Only 2% of enterprises using firewalls. Some enterprises utilized advanced security technologies such as intrusion detection systems (21%) and web filters (15%).

One of the major arguments for insufficient information security in enterprises is a lack of responsible personnel within the enterprises. This results in a lack of responsibility for information security inside the organizations. The management of the organization still seems to disregard the risks of security attacks. In most enterprises, network administrative personnel seem to take the ultimate responsibility for information security. Among the respondents, more than a half of the enterprises (56% in the country, 61.6% of enterprises in the south, 51.5% of enterprises in the north) had personnel responsible (either direct or indirect) for information security. (See Figure 2-4-7).

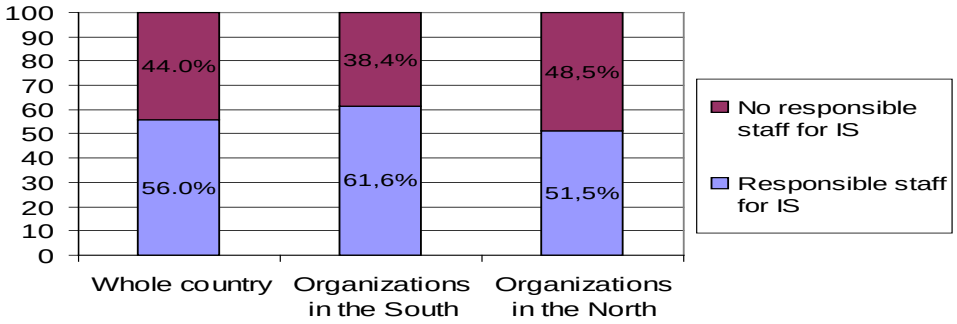


Figure 2-4-7 Percentage of companies with personnel responsible for IS (direct and indirect)

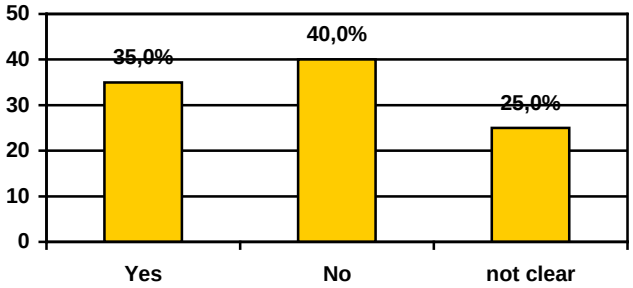


Figure 2-4-8 Percentage of companies that could identify the attacks

The lack of expertise resulted in insufficient knowledge of attacks. Only 35% of respondents could identify the attacks, 40% could not, and 25% were unaware of the attacks. Accordingly, only 29.7% of respondents could estimate the financial loss from the attacks, while 70.3% could not (Figure 2-4-9).

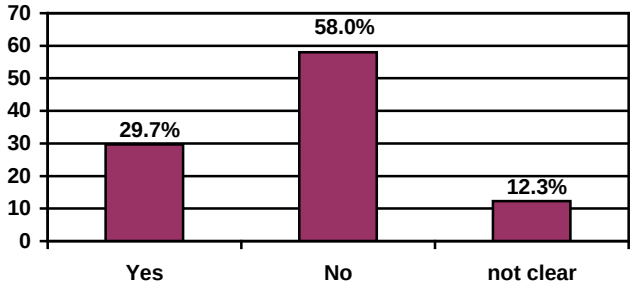


Figure 2-4-9 Percentage of companies that could estimate the financial loss due to attacks

The international standard ISO/IEC 27001 is an accepted worldwide standard, covering information security management. Among the respondents, 19.4% have a plan to implement ISO/IEC 27001, 50% have plans for other standards, and 30.6% do not know about any standard.

The investment in information security is expected to increase. More than 58.7% of respondents assume that increased investment in information security is necessary, only 26% think it will decrease, and 15.3% are not clear (Figure 2-4-10).

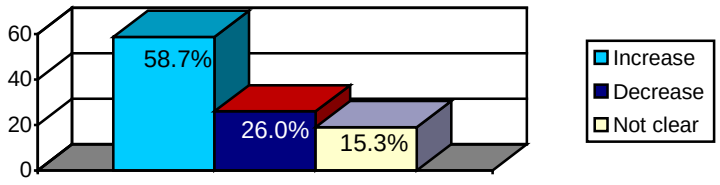


Figure 2-4-10 Opinion of companies on financing investment for IS

Realizing the importance of information security, many companies had taken part in many national programs and activities, such as awareness improving courses in Hanoi, Da Nang and Ho Chi Minh City in the years 2006, 2007, and 2008. Some other specific courses are for building CSIRTs, implementing ISO/IEC 27001, and IS management guidelines. The Vietnam Information Security Association (VNISA) was established in November 2007 and has gained much attention in society. However, companies still realize several remaining issues, especially the deficit in awareness by users, the deficient awareness of the organization, and the deficient support of company leaders (see Figure 2-4-11).

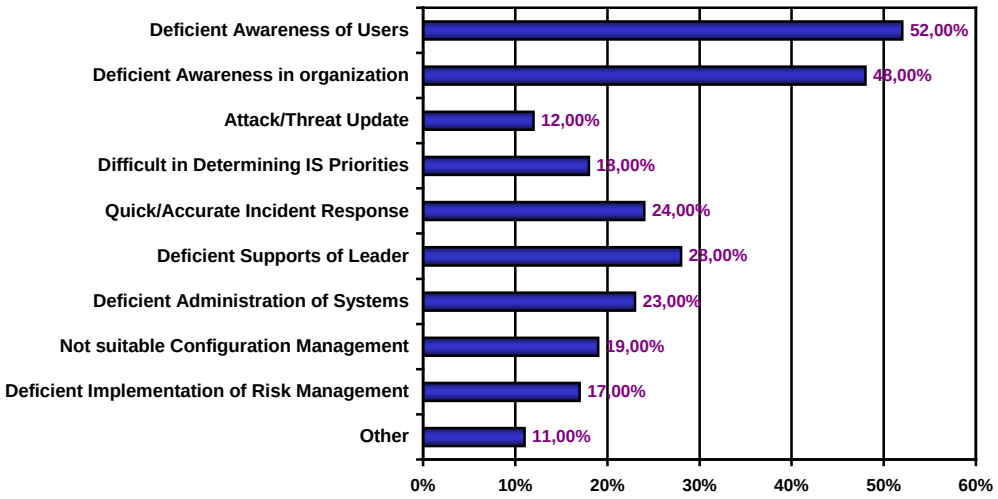


Figure 2-4-11 Challenges in the practice

All companies face the challenge of IS. This is essential for companies to understand the risk and threats to confidentiality, integrity, and availability of company information and computer systems. Companies should require a high level of security countermeasures.

(2) Government Policies Related to the Business Sector

The government of Vietnam is aware of the important role of the business sector, especially SMEs in the economic-social development of the country. Vietnam has been implementing a large number of measures to further encourage and support the development of the business sector, including the enterprises law, the investment law, the competition law, the anti-monopoly law, and the bankruptcy law.

Governmental support programs for SMEs are identified in Decree 90/2001/ND-CP, including financial support programs, technical support programs, international cooperation support, and programs for support and risk investment funding. Moreover, several human resource training programs for the business sector and SMEs have been promulgated in the finance budget in Decision 1347/2004/QD-BKH and Circular 09/2005/TT-BTC. Resolution 14/NQ-TW 2002, Decision 94/2002/QD-TTg, and Decision 236/2006/QD-TTg presented the development plan and main orientations for SME.

The growth of IS issues has prompted legislatures to take action. The Criminal Law (1999) identified the new type of cybercrimes. The IT Law (2006) illustrated three groups of cyber criminal acts. The e-Transaction Law (2005) went into effect in 2006 with regulations on legal data and addressed the use of legal documents and data, digital signatures, certificate authentication, e-transaction security, and personal data secrets. The Ordinance on Post and Telecommunications issued in 2002 established regulations on protecting ICT infrastructure and information security.

The Vietnamese government recently issued a number of decrees and regulations related to information security. Decree 160/2004/ND-CP detailed the requirements for assurance of safety for telecommunication networks and IS. Decree 57/2006/ND-CP is for e-commerce. Decree 64/2007/ND-CP is for security of ICT applications. Decree 97/2008/ND-CP was recently issued and replaced the obsolete Decree 55/2001/ND-CP for Internet regulations. Direction 03/2007/CT-BBCVT requires companies and organizations to protect their operations on the Internet. Decree 90/2008/ND-CP established standards for anti-spam and requires companies to control mail and message spam. Joint-Circular 06/2008/TTLT-BTTTT-BCA issued detailed regulations on IS and protecting the information infrastructure.

Accordingly, the most widely accepted standard, ISO/IEC 17799, was translated and renumbered into the national standard TCVN-7562:2005 to provide general guidance for IS system requirements, risk management, measurement, and implementation. The national standard TCVN 27001:2008 was translated to align with the ISO/IEC 27001 standard. TCVN 15408 and TCVN 18045, which correspond to ISO/IEC 15408 and ISO/IEC 18045 respectively, are waiting for approval.

As concerns about the demand of IS continues to grow, more attention and action by legislators and regulators have been acknowledged.

(3) Study on Information Security Management Benchmark

Various opinions, both in the business sector and in government, have been given regarding the issue of IS management. There is a broad consensus among companies and organizations as to the kinds of measures that should be undertaken by organizations. A common ISM benchmark for IS assessment is a basic necessity.

To better understand the IS status and the implementation of IS measures in the business sector in Vietnam, a study on ISM benchmark was planned from December 2008 to January 2009. The purpose of this study was to monitor the current IS status in the business sector in Vietnam, to obtain opinions on the need and roles of the common ISM benchmark, and to study possible national specific issues by implementing the ISM benchmark. The expected survey results should provide answers to the following questions:

- How well can the ISM benchmark assess a company's IS measures?
- How many respondents are willing to use the common ISM benchmark?
- Does the ISM benchmark reflect all the need of companies in assessing the IS level?
- Which issues of the common ISM benchmark can be seen from actual users regarding the country's specific issues?

Target samples were domestic companies or government-linked companies that utilized computers and networking. Respondents were selected from various industries, including: Information services (three companies), manufacturing (three), telecom (four), finance and insurance (one), broadcasting (one), publishing/newspapers (one), and public welfare (one). A fair balance of eight SMEs with less than 300 employees (with 10, 40, 50, 65, 100, 120, 200, and 200 employees), three middle to large companies with 300-1000 employees (with 500, 600, and 600 employees), and three large companies with more than 1000 employees (with 3000, 10,000, and 90,000 employees) was adopted (see Figure 2-4-12, Figure 2-4-13). Selected companies represented three groups: 65% in group I (high level IT security measures required) with nine companies, 14% in group II (medium level IT security measures) with two companies, and 21% in group III (no thorough IT security measures required) with three companies.

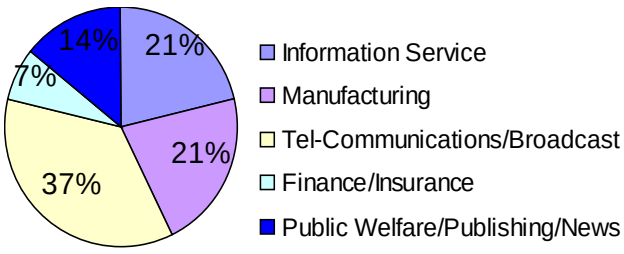


Figure 2-4-12 Classification of companies based on industry branches

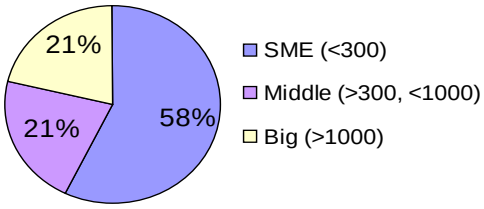


Figure 2-4-13 Classification by the size of organizations

Due to the specific form and different development of areas in Vietnam, the following sample units were adopted: three large nationwide companies, seven companies in the north, two companies in the middle, and two companies in the south. Respondents were selected from either IT managers or people who took care of computer and network systems, but not necessarily as the representative of the company. They should understand IS. However, due to the lack of expertise and experience with the ISM benchmark, detailed guidance should be provided.

As the first step, a printout of questionnaires and a user guide were sent to respondents via e-mail. The respondents were required to study the questionnaires, prepare the answers, and respond to the questionnaires on the website of IPA[10]. The answers from the respondents and assessment results were gathered by e-mail for further analysis.

According to the answers from the companies and the results and scores provided by IPA's website, we can summarize the assessment results as follows.

Major findings

Figures from 2-4-14 to 2-4-16 showed the total average score for all companies in group I, group II, and group III, respectively, in comparison with the average and desired level of 2165 records provided by IPA. In Figure 2-4-14, two companies achieved the desired level of total scores, four companies were around the average level, and three companies were below the average level. The total average score of all G1 companies was 80, the average score on each questionnaire was 3.2.

[10] http://www.ipa.go.jp/security/english/benchmark_system.html

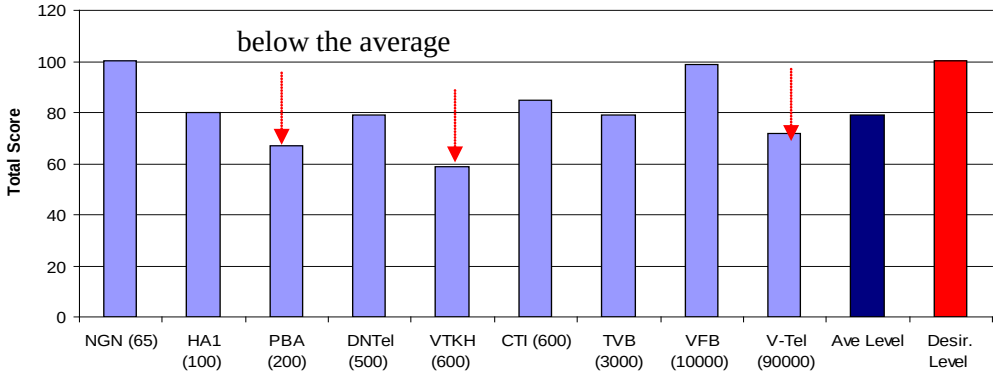


Figure 2-4-14 Total average score for all companies in group I

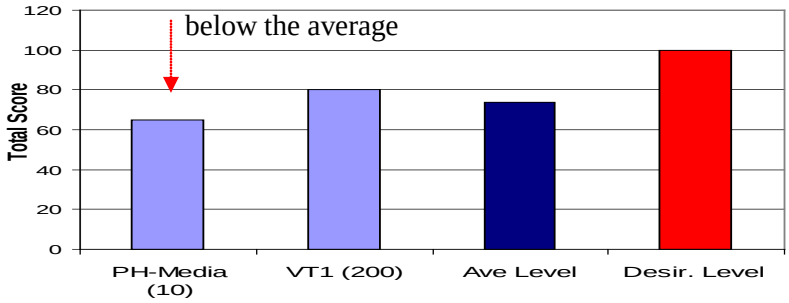


Figure 2-4-15 Total average score for companies in group II

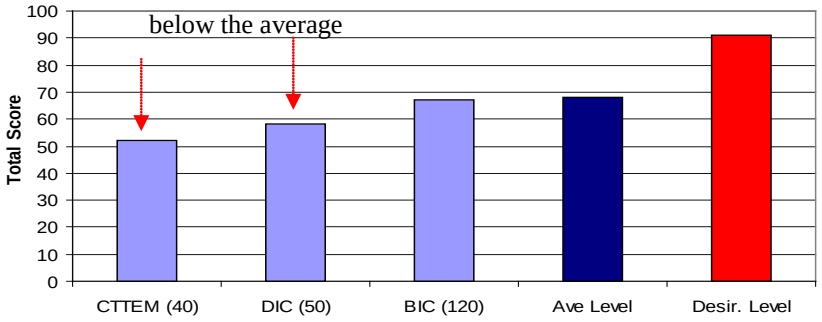


Figure 2-4-16 Total average score for companies in group III

Figure 2-4-15 showed the total score of two companies in group II in comparison with the average and desired level of IPA. The total average score of two companies was 72.5, the average score was 2.4 for all questions. Similarly, Figure 2-4-16 showed the total score for three companies in group III compared with the average and desired level of IPA. The total average score of three companies was 59.0, and the average score was 2.4 for all questions.

For further analysis of 25 items on information security measures, an average score rating for each of 25 questionnaires is given in Figure 2-4-17. The figure showed a deficiency in security training and software management of companies in group I because the percentage of scores below the average was large than the percentage of scores above the average. Figure 2-4-18 presented the corresponding score rating for all companies in three groups and the deficiencies in several items.

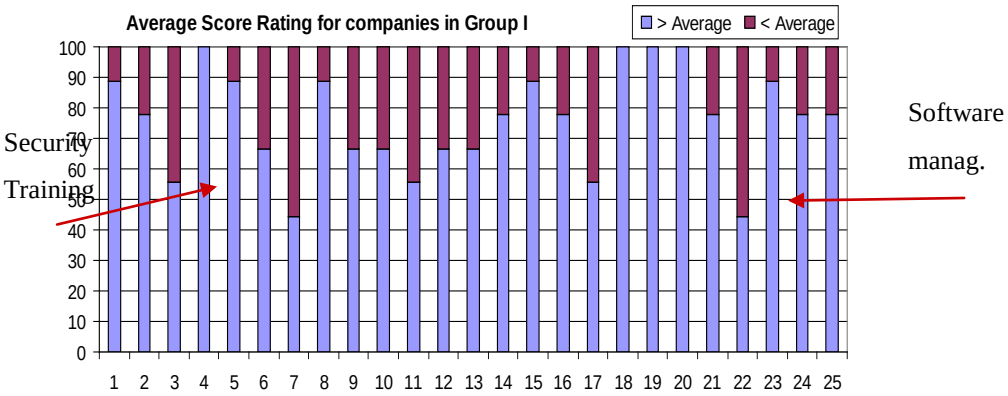


Figure 2-4-17 Average score rating for companies in group I

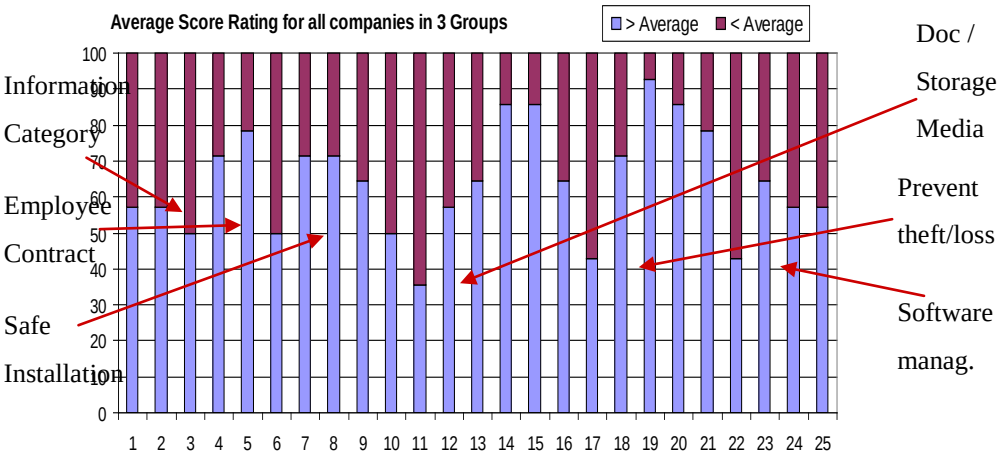


Figure 2-4-18 Average score rating for all three groups

As shown in the Figures, it was found that group I companies were more proactive in IS measures, since they had fewer deficiencies than all companies in the three groups. The total average scores of SMEs (less than 300 employees) in corresponding groups are shown in Table 2-4-2 compared with 306 records provided by IPA.

Table 2-4-2. Total average scores of SMEs compared with 306 records of IPA

Companies	Total average score	Average score for all questions	Average Level by IPA	Average Score by IPA	Desired Level by IPA	Desired Score by IPA
Group I- SMEs	82.3	3.3	79	3.2	100	4.0
Group II- SMEs	72.5	2.4	74	3.0	100	3.8
Group III- SMEs	59	2.4	68	2.7	91	3.7

Overall, SMEs in group I were more protective than SMEs in other groups. SMEs in groups II and III still had a low security level and lack IS measures to protect their systems. On the other hand, SMEs were better prepared for IS measures than large companies. One main reason was the deficient awareness of employees and large companies. The comparison of the total average score of large companies belonging to group I with 859 records provided by IPA is shown in the Table 2-4-3.

. Table 2-4-3 Total average scores of large companies compared with 859 records of IPA

	Average score of large companies in GI								
Companies	DN-Tel	VT-KH	CTI	TVB	VNB	V-Tel	Aver. Score	Aver. Level by IPA	Desir. Score by IPA
Total score	100	80	67	79	99	72	**82.8**	84	102
Ave. score of all questions	4.0	3.2	2.7	3.2	4.0	2.9	**3.3**	3.4	4.1

Large companies faced major challenges in several IS measures. The percentages of large companies with scores below average regarding 25 IS measures were in security policy (50%), security organization (50%), information categorization (50%), security training (68%), document/storage media (68%), operation environment (50%), IT system operation (68%), prevention of theft/loss (50%), and security incidents (68%). Most large companies were very good at data access control.

Based on industrial sectors, the percentage of companies with scores below average regarding 25 IS measures were indicated in the Figures from 2-4-19 to 2-4-22. The analysis indicated that information services companies were better than other industrial sectors. The awareness of IS in manufacturing companies was very low. These companies were lacking in many IS measures.

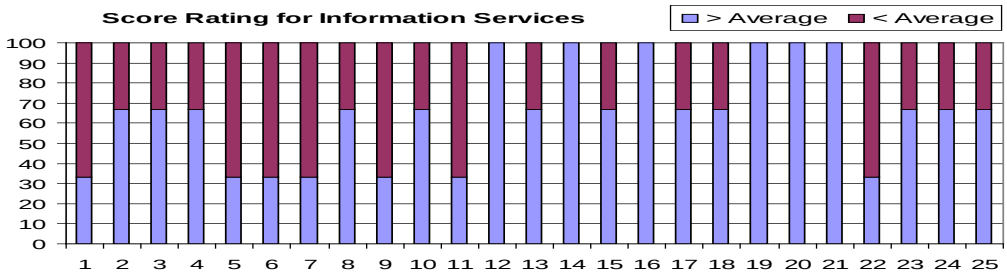


Figure 2-4-19 Score rating for information services

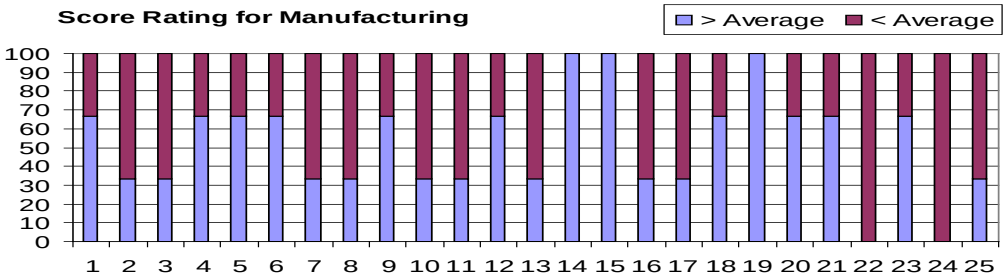


Figure 2-4-20 Score rating for manufacturing

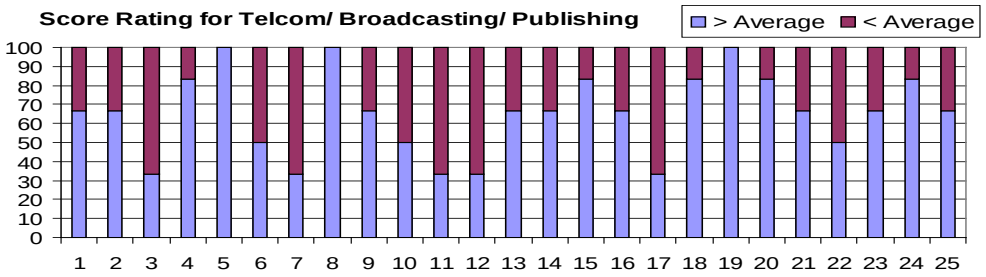


Figure 2-4-21 Score rating for Telcom/Broadcasting/Publishing

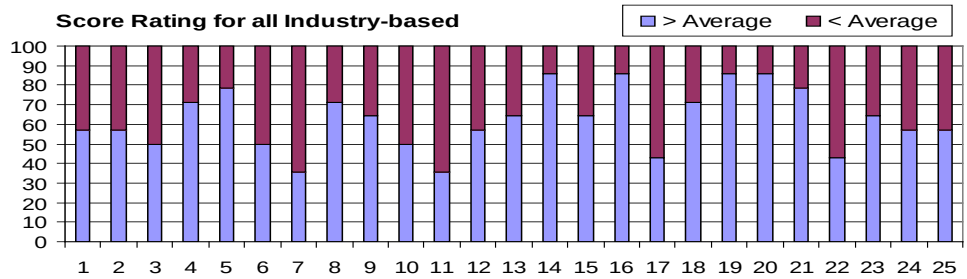


Figure 2-4-22 Score rating for all industries

Table 2-4-4 is a summary for the groups classified by industry and by the size of companies in comparison with 1688 records provided by IPA.

Table 2-4-4 Total average scores of all companies compared with 1688 records of IPA

	Group A (Classified by Industry)		Group B (Classified by Industry and then by company's Size)				Diff. in Ave. Total Scores
			SME companies		Large companies		
	Total Score	IPA Ave.	Total Score	IPA Ave.	Total Score	IPA Ave.	
Information Services	76,67	82,84	72,50	79,58	85,00	87,99	12,50
Manufacturer	66,33	71,65	66,33	65,32		77,41	0
Telecom /Broadcast/ Publishing	76,00	82,84	83,50	79,58	72,25	87,99	11,25
Finance/Insurance	99,00	78,45		75,70	99,00	83,23	0

Beside of 41 questions on the IPA website, companies were asked to provide answer six additional questions about their opinions on the ISM benchmark. The answers from 14 companies were reviewed and analyzed.

A positive reaction from companies was that all of 14 companies thought that the ISM benchmark was very useful and effective in assessing their company's IS level. This was because the ISM benchmark is practical and could give them information about the IS level in the company. All 14 companies thought that the ISM benchmark helped them to know more about the problem domains of IS and to obtain more advice about IS measures. Feedback from companies indicated that they were very concerned about attacks and often had problems with IT security, but they did not know the problem domain and did not know how to improve the IS level within their company. All 14 companies believed that the ISM benchmark had given a good assessment of the IS level within their organizations and helped them to compare the IS level with the average.

Most companies (13 of 14) are willing to use this ISM benchmark in their company to check the IS level. The reasons were that the ISM benchmark is a free, effective, and easy-to-use tool to assess the IS level of companies, to identify the IS problems in companies, to compare the IS level with other companies in Japan, and to know which IS measures should be improved within their companies. However, no company wants to use the ISM for checking the supplier's IS level. Among the 14 companies, 8 want to report their IS level to clients. One company was not willing to use the ISM benchmark because they thought that this self-diagnostic was still general and

did not have detailed explanations on practical use. They want to have additional questionnaires, more functions need to be added, and more information on the assessment results. Actually, the ISM benchmark is a good tool. However, some users were of the opinion that several questions were difficult. Although the respondents were CIO or personnel responsible for IT security within the companies, they still did not know details on information security standards such as ISO/IEC 27001. Thus, some of them said that sometimes it was difficult to answer specific questions. Maybe it was a problem with the English language as well. On the other hand, some terminologies were new for users and not typically used in Vietnamese companies such as business continuity, risk assessment, etc. That was why most companies indicated a deficiency in awareness security training and IS management as shown in Figure 2-4-11 in the previous section. In this figure, 52% of companies showed deficient awareness by users and 43% of companies indicated deficient awareness within the organization.

All 14 companies responded that the ISM benchmark was easy to use due to the user-friendly and website-based structure of the benchmark, the output graphical results, and the good tips and hints for answering the questions. The assessment process was simple and provided quick output results. The questions covered all aspects of organizational, technical, physical, environmental, and human security measures in a good balance following the Plan-Do-Check-Act style of the ISO/IEC 27001.

According to the answers from the respondents, the ISM benchmark covered five essential sections of IS corresponding to the basic requirements of IS management at a high level. It reflected the rapid changes in the IS environment of the organizations. Basically, the existing functions of the ISM benchmark already met the need of companies for IS level assessment. Nevertheless, depending on survey questionnaires in recent years and based on the additional need for further analysis, the respondents provided several ideas about possible additional functions and improvements for the ISM benchmark.

Among the 14 respondents, 6 suggested additional functions for improvement of the ISM benchmark, and 8 had no comments. More questionnaires on human resource requirements and the type of protection equipment were suggested in order to indicate detailed measures and the appropriate level for each company. Comparisons between different

departments within a company were also desired. On the other hand, further information representing assessment and comparison results were expected. Respondents wanted to have more information on calculation of the information security risk index and T-score in order to represent the detailed IS level. Some companies reported a difficult connection to the IPA server during the survey. Thus, they suggested that it was necessary to improve the functionality and the load on the IPA server in case of a large number of connections. One idea was the proposal for a local server and a local analysis of the results.

Regarding the implementation of IS measures within business partners, the respondents had to answer two questions in the survey. Of 14 companies, 7 companies had requests to implement IS measures from business partners and 7 said “no”. Five of the 14 companies had requested implementation of IS measures by business partners, while 9 companies had no comments. Some standards requested by business partners were ISO 27001, PCI, VPN, ISO 17799, and some company’s standards. These results also showed that some of the IS standards, such as ISO 27001, are being implemented in the business sector in Vietnam by direct application of international standards in some organizations.

(4) Need for International Common ISM Benchmark

The answers of respondents showed an evidence for the need for a common ISM benchmark. Considering the rapid demand for IS level assessment in the business sector and the lack of an assessment tool, all of the companies in this study (14/14) thought that a common ISM benchmark was urgently needed.

All companies in the survey (14/14) answered that the ISM benchmark was effective, useful, and suitable in assessing their IS levels. Companies could use the ISM benchmark to check the company’s IS level, to identify the IS problems in the company, to obtain advice about necessary IS measures, to identify the deficiencies and the areas for improvement, to compare their company’s IS level with the average (either with international companies or other domestic companies), and to be able to report their IS level to clients and customers. Most companies (13/14) were willing to use the ISM benchmark in their companies. Only one company was in doubt about the secure connection to the IPA server by sending company profiles.

The business performance, the demands of FDI, out-sourcing, and off-shoring projects had prompted implementation of IS measures in the business sector and the mutual acceptance of the IS level. The role and significance of a common ISM benchmark are clear in expansion of direct investment and outsourcing.

From the point of view of companies, a common ISM benchmark is useful in providing evidence on IS levels of mutual partners, to show the deficiency and necessary improvements of IS measures in order to meet the desired level of mutual acceptance in corresponding industries, to prepare appropriate investments since security risks were clearly understood, and to build trust between companies/clients/customers for direct investment and outsourcing contracts. Assessment of IS level for companies and organizations is now an urgent demand.

In order to realize a practical and powerful common ISM benchmark, several aspects have to be considered. The common ISM benchmark should be easy-to-use and user-friendly. According to the survey, all of the companies (14/14) remarked that the ISM benchmark was very easy to use as it was at a high level and did not require specific knowledge. The design of the common ISM benchmark should be simple but effective. It should give good tips and guidelines for answering the questionnaires.

However, by testing the ISM benchmark provided by IPA, companies were of the opinion that several additional functions would be expected as mentioned in the previous section. Actually, the ISM benchmark was still at a high level of assessment. A real practical demand was the requirement of quantitative versus qualitative results. Some detailed items on IS measures were also required.

With respect to the need for additional functions, multiple issues could be seen and should be considered by development of an international common ISM benchmark. First is the effective balance between the long list of questions and the desire for adding more checks. Many users wanted to add more questions to check on detailed items such as the use of protective equipment, the percentage of responsible personnel, and other factors. One idea was to customize the common ISM benchmark according to the business sectors or the type of users depending on need for IS levels. Additional questions might be on detailed items for further analysis. Second is effective functionality and load on the server. Third is the additional information on the

output results and additional hints for users. All additional functions also represented the desire for an international common ISM benchmark.

The business sector has made a significant contribution to economic reform and economic development in Vietnam, as already mentioned in section (1). As ICT has been an engine driving the business sector, IS issues are being considered as an essential factor in business operations, especially in the development of e-commerce, e-government and promotion of FDI projects, international out-sourcing, and offshoring contracts. The Vietnamese government already acknowledged this need and committed to take more action represented by a number of policies (see section 2). However, a broad consensus is the lack of an assessment benchmark that the business sector can readily adopt. The common ISM benchmark is a tool that could entail the company's oversight and execution of IS measures in the business sector.

An international common ISM benchmark is important because it provides a roadmap for the implementation, assessment, and improvement of IS measures within companies and organizations. A company that uses this benchmark can assess its IS level over time, determine the need for additional measures, and improve its IS level through visualization of the risks. Moreover, the common ISM benchmark helps to build a mutual trustworthy partnership of companies for promoting more foreign direct investment and outsourcing contracts in the region.

2.5. China

(1) Current Status of Information Security in Business Sector in China

In recent years, information technology has developed rapidly and been applied widely in the business sector in China. According to the 23rd Survey Report on China Internet Development Status,[11] which was issued by the China Internet Network Information Center (CNNIC) on January 13, 2009, the number of Internet users in China reached 298 million by the end of 2008, and the Internet penetration in China has risen to 22.6%, slightly higher than the world's average of 21.9%. The CNNIC survey results also show that e-commerce developed rapidly in China in 2008, and that e-commerce penetration jumped 60% to 24.8% from the previous year.

[11] http://www.cnnic.org.cn/uploadfiles/pdf/2009/1/13/92458.pdf

The rapid development and wide application of information technology brings many benefits to the China business sector, and it also causes many information security problems; such as the flood of computer viruses, trojan horses, and other malicious software; hacking and cracking; and the theft of trade secrets via Internet espionage. All of these represent a serious threat to the confidentiality, integrity, and availability of information assets of the business sector and, consequently, threaten the existence and development of business.

At present, information security incidents occur frequently in the business sector in China. According to 2008 Survey Report on Network Security and Computer Virus Epidemic,[12] which was issued by the Ministry of Public Security of the People's Republic of China (MPS) on October 20, 2008, 62.7% respondents had information security incidents in the last year, and the computer virus infection rate was 85.5%. These incidents cause business sector system failure, data corruption or loss, unauthorized remote access, and stolen user accounts and passwords. The status of computer virus infection in China in the most recent eight years issued by MPS is illustrated in figure 2-5-1. The MPS survey results show that information security in the business sector in China is still serious currently.

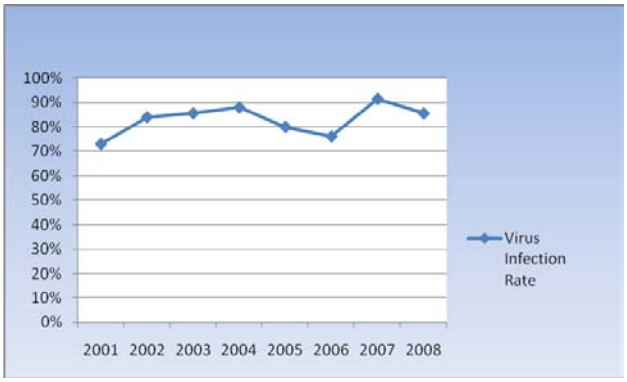


Figure 2-5-1 Computer virus infection in China in recent 8 years

Another survey report, which was carried out by E-Works[13] for Chinese manufacturing information security in 2007, shows that nearly half (48.5%) of the enterprises are not satisfied with the current status of their information

[12] http://www.antivirus-china.org.cn/head/diaocha2008/xinwengao2008.htm

[13] http://www.e-works.net.cn/report/safereport/safereport.htm

security. Only 1% of the total enterprises surveyed did not have any information security incident during the past three months. The survey results also show that the major information security challenges to the enterprises are from lack of information security awareness, inadequate investment on security, lack of security policies, insufficient functions of information security products, and lack of security professional personnel or lack of security training (see figure 2-5-2). Security awareness and investment are the greatest challenges.

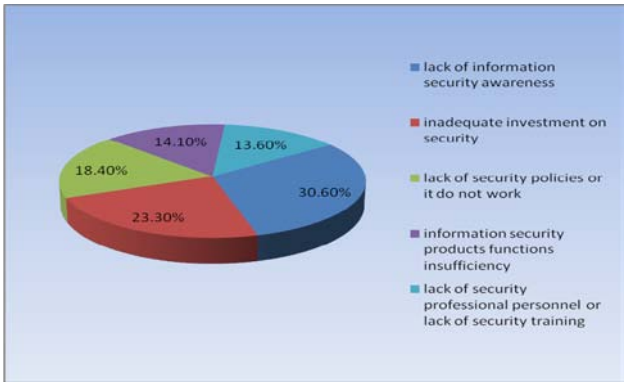


Figure 2-5-2 Information security challenges to the enterprises

In conclusion, the current information security problem in the business sector has become one of the crucial risks that impact business. The government agencies and the business sector itself should really do something to address information security issues to protect and promote business development.

(2) Government Policies Related to the Business Sector

Chinese government agencies have attached great importance to information security issues. Since the 1990s, China has promulgated a number of governmental policies and a series of national information security standards to support and promote business sector to solve information security problems. As of December 31, 2008, the information security regulations and standards published by China are shown in Table 2-5-1.

Table 2-5-1 Number of Regulations and Standards

Items	Regulations	National Standards
Number	16	63

For the security protection of computer information systems and the promotion of the application and development of computers, the State Council promulgated the People's Republic of China Computer Information System Security Protection Ordinance (CISSPO) in 1994. As the first information security law, it stipulates that any organization or individual shall not use the computer information system to endanger national interests, collective interests, and the legitimate interests of citizens and shall not endanger the safety of computer information system. The law also stipulates that Classified Protection of Information Security (CPIS) shall be taken to protect computer information systems.

The CPIS is a main policy of information security protection in China. According to the CISSPO, the MPS issued a Regulation of Classified Protection of Information Security (RCPIS) associated with other government agencies in 2007. Meanwhile, China published a series of national standards related to CPIS, such as the following:

- GB/T22019 Requirements of Classified Protection of Information Systems Security
- GB/T22020 Classification Guide for Classified Protection of Information Systems Security

According to RCPIS, The information security of an organization is classified into five levels, organizations should define first what level they should be based on relative to the national standard of GB/T22020, and then they shall implement measures to protect information systems in accordance with the relevant requirements from the national standard of GB/T22019. Organizations with three levels or higher should be tested and evaluated by a third party at planned intervals to determine whether they meet the relevant basic requirements from GB/T22019.

Another governmental policy related to the business sector is Information Security Management System (ISMS) certification based on ISO/IEC27001.

More and more organizations are interested in ISMS certification in China since 2000. Around two hundred organizations have received the ISMS certificate. In 2008, China published a series of ISMS national standards, such as the following:

- GB/T22080 ISMS Requirements (ISO/IEC 27001:2005, IDT)
- GB/T22081 Code of practice for ISM(ISO/IEC 27002:2005, IDT)

Meanwhile, the Ministry of Commerce of the People's Republic of China launched a program to promote ISMS certification for the service outsourcing sector. According to this program, the government can provide financial support to the organizations that have received the ISMS certificate.

(3) Study on Information Security Management Benchmark

i) Overview of this study

According to the survey method designed by ERIA WG1, six China domestic enterprises selected to use the ISM benchmark system provided by IPA and answered the questionnaire from January 15, 2009 to February 14, 2009. Table 2-5-2 shows the details of the respondents.

Table 2-5-2 Attributes of Respondents

Size	Number/Ratio	Type of Industry
Large	3 / 50%	Internet Gaming, HR Service, Information Security Product Developing
SMB	3 / 50%	Information Service, Software Evaluating and Testing, Credit Card Manufacturing

According to the ISM benchmark system reports sent back by the respondents, the Total Scores of the six respondents were all lower than the

ideal security level suggested by the system. It indicated that the information security level of the respondents should be improved. Figure 2-5-3 shows the total score of the six respondents(S for SMB, L for Large).

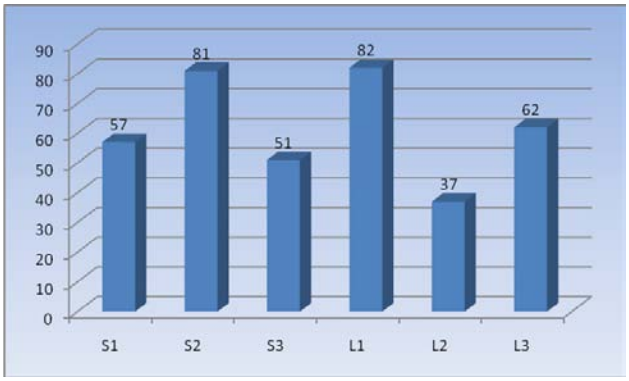


Figure 2-5-3 The Total Score of the 6 Respondents

ii) Analysis of the needs for the ISM benchmark

According to the results from Q1 and Q2, a common ISM benchmark is needed in the China business sector. All of the respondents answered that the ISM benchmark was effective in assessing their information security level, and 83% of respondents answered that they were willing to use the ISM benchmark (see table 2-5-3).

Table 2-5-3 the results to Q1 and Q2

Question	Yes Answer	No Answer
Q1	100%	0%
Q2	83%	17%

Most of the respondents thought that the ISM benchmark was effective in determining their information security problems, to obtain advice about information security measures, and to compare the information security level with the average. Seventeen percent of respondents considered that the ISM benchmark was too general to use.

iii) Analysis of the expected functions for the ISM benchmark

According to the results of Q3 and Q4, the functions of the ISM benchmark basically met the needs of the business sector for measuring their information security level.

All of the respondents answered that the ISM benchmark was easy to use, and 17% of respondents commented about the result output, but they did not provide any ideas (see table 2-5-4).

Table 2-5-4 the results to Q3 and Q4

Question	Yes Answer	No Answer
Q3	100%	0%
Q4	83%	17%

iv) Analysis of the roles for the ISM benchmark

The results for Q5 and Q6 show that 33% of the respondents have been asked for information security measures by their business partners, and 17% of respondents had requested information security measures by their business partners (see table 2-5-5). The standards they had been asked or had requested compliance were ISO/IEC2700x and SSE-CMM.

Table 2-5-5 the Results to Q5 and Q6

Question	Yes Answer	No Answer
Q5	33%	67%
Q6	17%	83%

Only according to the answers to Q5 and Q6, we are not sure what role of the ISM benchmark in the business sector in China. But implementation of some of the information security measures, such as ISO/IEC2700x, SSE-CMM, have been requested by business partners.

v) Issues

The sample size of this survey is too small, and the survey results do not always reflect the reality of the Common ISM Benchmark in China. There are some issues in realizing the common ISM benchmark, although the survey results show that the ISM benchmark is needed, effective, suitable, and easy to use in the business sector in China, such as the following:

a. How to deal with the relationship of the common ISM benchmark and other information security protection projects, such as ISMS, the classified protection of information security, to enable it to be accepted by the business sector, and to be supported by the government in China.

b. How to realize the comparability of the common ISM benchmark assessment results with other information security measurement systems, such as ISMS auditing, the classified protection of information security evaluations, and testing.

c. How to localize the common ISM benchmark system in China, including the system server and system language.

d. How to promote the common ISM benchmark to enable more companies and individual to know, trust, and use it.

(4) Need for Common ISM Benchmark

Based on the results of the study on ISM benchmark operated by IPA, we think that a Common ISM Benchmark should be established in Asia, which can provide the acceptable and comparable indicators of the information security management level of organizations, in order to build confidence between the business parties, to promote economic development in the Asian region.

2.6. Japan

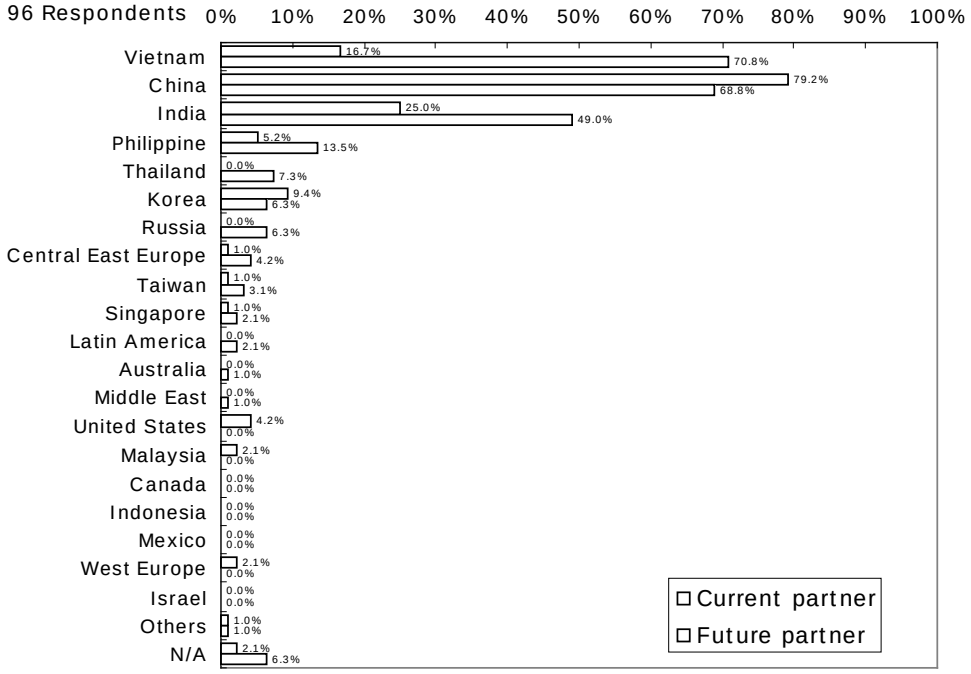
(1) Current Status of Information Security in Business Sector in Japan

i) Circumstances surrounding the business sector

More and more companies have implemented offshore outsourcing in order to reduce development costs, make up for shortages in human

resources, and complement the high use of overseas technical strength in Japan. IT outsourcing (ITO), such as software development and business process outsourcing (BPO) in which the functions of the indirect departments of a company are moved outside the company, have entered the mainstream as well as the conventional outsourcing by manufacturers. The report titled “Study on development and influence of offshoring” conducted by the MIC revealed that 38.6% of Japanese companies operating software development services (commissioned software development, software product development, and embedded software development) had performed offshore outsourcing, and the ratio was 40.6% when companies scheduled to develop software in the future are included.

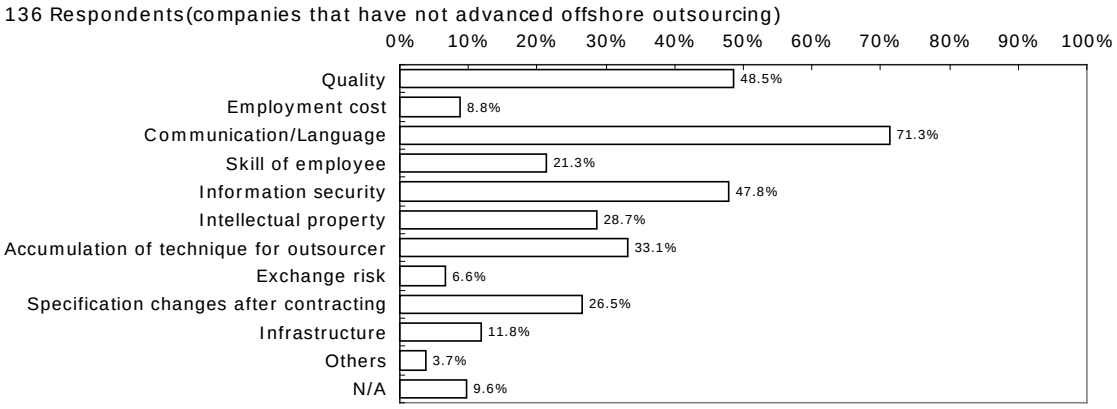
According to the results of this survey, China was the greatest partner country among other counterparts as an offshore outsourcing target, and 79.2% of Japanese companies outsourced offshore. India (25.0%), Vietnam (16.7%), and Korea (9.4%) followed. The ratios of outsourcing in Asian countries were overwhelmingly high. As promising countries for offshore development outsourcing, Vietnam and India ranked high, which was included in the results. Demand for Asian countries as outsourcees remains high.



Source: MIC, “Study on development and influence of offshoring ” (2007)

Figure 2-6-1 Current and future offshore development partner countries and regions

Meanwhile, there are many companies that have not advanced offshore outsourcing yet. According to this survey, they responded that anxiety about information security (47.8%) as the second issue yet to resolve for offshore development after linguistic problems (71.3%) and anxiety about quality (48.5%). From these results, we can see that anxiety about information security is one of the impediments to expanding offshore outsourcing.



Source: MIC, “Study on development and influence of offshoring” (2007)

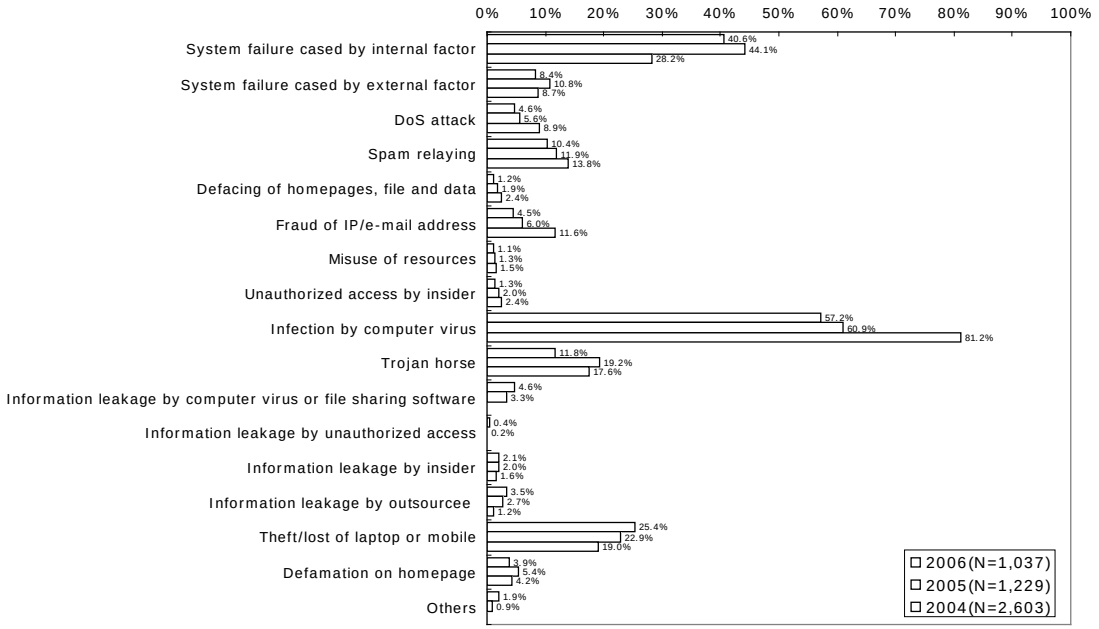
Figure 2-6-2 Challenges in advancing offshore development

ii) Situation of information security problems in the business sector

The Survey on Information Processing (2006) conducted by the METI in 2007 for companies revealed the whole occurrence of information security problems in Japanese companies had been decreasing while the incidence of confidential information leaks, such as theft and loss of laptop PCs and mobile storage media, had been increasing for three consecutive years. The survey conducted in 2004 showed that 81.2% of companies suffered from computer virus infections while the ratio had decreased to 57.2% by 2006. Consequently, the tolerance of Japanese companies for technological attacks has been steadily developing. Meanwhile, the percentages of all items related to information leaks have been increasing for three consecutive years. In particular, the percentage of theft and loss of PCs and mobile storage media is as high as 25.4%.

Since the personal information protection law took effect in 2005, leaks of private information by companies have been recognized as a social problem.

In particular, leaks of enterprise confidential information due to loss of laptop PCs by employees have been recognized as a major risk. Against this problem, companies have been considering and implementing different measures on technological and systemic levels. These days, there are information leaks involving industrial spies where technological and private information is intentionally stolen, which puts enterprise information management to the test again.



Source: METI, "Survey on Information Processing" (2008)

Figure 2-6-3 Occurrence of information security problems

iii) Situation of information security measures in the business sector

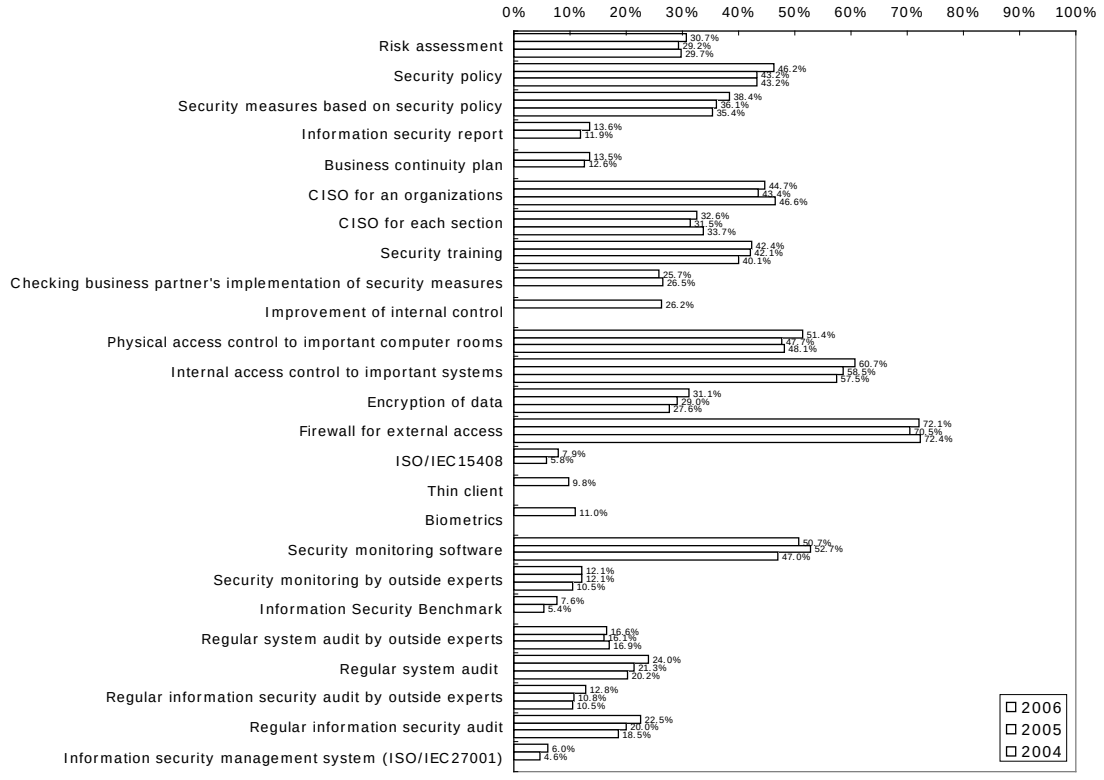
As can be guessed from the occurrence of information security problems, the implementation of technological measures by companies has made steady progress every year. Meanwhile, the ratio of organizational measures, such as establishing security policies and appointing a security administrator, is less than 50% for all items. Consequently, we can see that enterprise rules and systems have not caught up with technological measures. Information security risks are highly likely to arise because only 25.7% of companies have implemented information security measures for contractors (outsourcees).

Now that a variety of different types of outsourcing are expanding, Japanese companies have more opportunities to provide confidential

information to their domestic and overseas outsourced business partners. In Japan, there have been many cases where outsourced business partners leaked information. Information security measures must be reexamined in light of the whole business of a company including outsourced partners.

Furthermore, as characteristic results from this survey, the ratios of items related to evaluating information security measures, such as audits and monitoring, are low. Though they increased from the previous levels, the rates of executing internal system audits as of 2006 and information security measures are only 24.0% and 22.5%, respectively. From these results, we can see “C” of the PDCA cycle to evaluate these measures does not work fully.

The ratio of utilization of the ISM benchmark provided by IPA in connection with the evaluation process for information security measures steadily increased from 5.4% in 2005 to 7.6% in 2006. As the needs of the enterprise are increasing, the needs of companies for tools to understand information security and their outsourcees are expected to increase.



Source: METI, “Survey on Information Processing” (2008)

Figure 2-6-4 Ratios of companies which have taken information security measures

(2) Government Policies Related to the Business Sector

The Information Security Policy Council, established under the IT strategy headquarters led by the prime minister, develops an information security basic strategy for the government of Japan. The National Information Security Center (NISC) established in the Cabinet Secretariat comprehensively reviews and fully coordinates information security measures promoted by each government department as the secretariat for the Information Security Policy Council to create a draft as the national strategy on information security measures. The METI is responsible for information security policies intended for the business sector.

In the Information Security Policy Council as a policymaking body of information security strategies in Japan, the First National Strategy on Information Security as a mid-and-long-term strategy for information security in Japan was announced in 2006. In this strategy, entities in the private and public sectors, including government agencies, local governments, critical infrastructures, businesses, and the individuals have combined their knowledge and worked to enable the use of IT, which has played an increasingly more important role in safety and security after information security became an area of policy that must be selectively focused on among other IT-related policies. Figure 2-6-5 shows the comprehensive framework of these efforts.

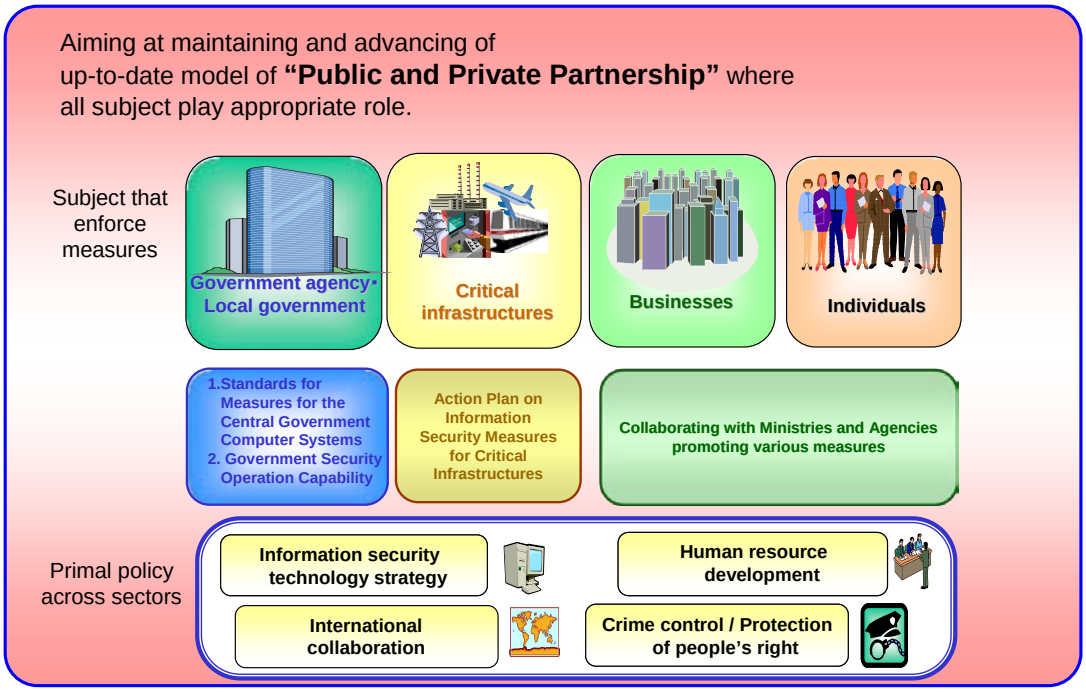


Figure 2-6-5 Comprehensive Framework of National Strategy on Information Security

This year, when the First National Strategy on Information Security expires, a new mid and long term strategy, the Second National Strategy on Information Security (Draft) for 2009 to 2011 will be announced.

The first strategy aimed "*improving the implementation of information security measures of businesses to the world's highest level*" and promoted efforts for that purpose. As one of the backgrounds to these efforts, efforts to avoid problems in information security in domestic and overseas business bases are required in order to facilitate global business development, such as offshore outsourcing, international inter-enterprise trade (supply chain), and foreign direct investment.

Then, the urgent issues identified in the Second National Strategy on Information Security is ensuring that business bases are safe and secure for Japanese companies with operations in foreign countries, strengthening information security measures for domestic companies in the global supply chain management, and promoting measures for small-and-mid-sized companies with strong international competitiveness especially in manufacturing. We are putting forth concrete efforts aiming at the following images in the information security efforts by Japanese companies in 2012:

Establishment of recognition as part of information security governance management and corresponding tools

Because the importance of information security governance varies depending on the level of utilization of information resources by companies, those with higher utilization levels and management fully understand the importance of information security measures and in-house security measures through external audits. Because the balance between costs and convenience is extremely important for these measures, the companies that provide products and services are aware of these elements, while the government and information-related companies that support these measures are actively promoting these measures.

Development of ensuring emergency response and business continuity to improve readiness for the "incident-assumed society"

As proactive measures for enterprise information security are developed, mainly major companies and those with greater importance of information security in business activities are stepping up reactive measures.

Development of appropriate measures in large and small-and-mid-sized companies

Appropriate and necessary measures have been implemented regardless of size, such as providing tools for small-and-mid-sized companies that have not implemented sufficient information security measures.

Development of information security measures in overseas bases of Japanese companies in any countries

The government of Japan and Japanese companies started implementing information security measures because of the full recognition of the importance of having no problems in information security, such as leaks of customer information, in their overseas business bases. In addition, sharing the importance of these efforts, the government of Japan and counterparts in countries where the bases are located are mounting efforts to improve the environment in which companies can use IT safely and securely by sharing the importance of these efforts with collaboration of the private and public sectors.

(3) Study on Information Security Management Benchmark

Since the IPA has started the ISM benchmark service in 2005 August in Japan, 3.5 years have passed. In these 3.5 years, various experiences have been learned and accumulated from the operation of the ISM benchmark.

In today's industrial world, it has become more common for enterprises to divide their labor into multiple units and assign them to their business partners or to outsource jobs to contractors. This situation often requires enterprises to provide technical information, trade secrets, and know-how to their business partners. In such cases, it is essential for them to ensure information security of their contractors. Frequent occurrence of information leakage and enforcement of the Private Information Protection Law prompted outsourcing companies to request contractors to implement information security measures. By implementing information security measures, enterprises can also gain competitive superiority.

NISC issued a standard for the government that can also be referred by the private sector. Clause 6.1.2 of the NISC standard says that the head of information security officers must establish procedures to evaluate information security level of their contractor based on international standard in order to select their contractor more rigorously. It means that security is one of the criteria for selecting contractors.

However, people might ask how and in which way they can evaluate their contractor’s security level. To answer this question, NISC issued guidelines on how to evaluate information security level of contractors. In the guidelines, NISC shows the following three assessment methods:

- ISM Conformity Assessment based on International Standard 27001
- ISM benchmark
- Information Security Audit

When requested by your business partner to report the current status of information security countermeasure implementations, you can use these methods. However, if the assessment cost is too high or the method requires expertise, assessment itself becomes a burden for the enterprises that don’t have enough recourse for Information Security. The ISM benchmark is a system that can solve such problems.

The ISM benchmark has the following characteristics:

1.Free web-based self-assessment tool

2. Requires no special knowledge as the number of questions regarding information security controls is limited to 25 and those questions are expressed using plain words.
3. Conforms to International Standards ISO/IEC 27001:2005 25 questions were derived from 133 security controls in Annex A of ISO/IEC 27001:2005. These questions cover information security controls that should be implemented by organizations, including organizational, physical, technical controls.
4. "Gateway" to assessment/certification by a third party because by using the ISM benchmark, you can check your organization's approach to information security more easily than using the ISMS Conformity Assessment or Information Security Audit.
5. Scalable, because the ISM benchmark provides 146 tips for 25 security controls and these tips can be used to perform more detailed assessments.
6. Reliable, because based on the concept proposed by METI, the government agency IPA developed and released this tool on its web site.

Regardless of the superb functionality of a tool, it will not be widely used by the public unless its existence and usability is made known to the public. Since 2005, METI has been holding the ISM benchmark Seminar on a regular basis. IPA held the information security seminar in all parts of Japan more than 30 times every year and demonstrates how the ISM benchmark works. We also contribute articles on the ISM benchmark to a variety of magazines.

The ISM benchmark can be used in the phases of developing and implementing information security controls as well as the operational phase to improve the information security level. You can also use it to check your level before undergoing the ISMS Conformity Assessment or Information Security Audit. In the past, this tool was not fully used as a multipurpose tool because there were no tips provided how to use this tool. To overcome this situation, experts[14] gathered to create a book called *The Handbook of*

[14] ISM Benchmark Handbook was written by IPA (which provides ISM Benchmark), JIPDEC (which conducts ISMS Conformity Assessment) and JASA (which conducts Information Security Audit).

the ISM Benchmark [15] so that people understand how to make use of it.

Figure 2-6-6 shows the number of those who used the ISM benchmark from August 2005 to January 2009 (by month). From the figure, we can see that the highest number was 1,148 in September 2006, followed by 913 in February 2007, and 895 in August 2005. September 2006 is the month the NISC guidelines were published, and February 2007 is the month the minister of METI requested government agencies to check their information security level using the ISM benchmark.

After checking the number of those who used the ISM benchmark for each month and what event took place in that month, we found the following three factors contributing to the increase in the use of the ISM benchmark.

1. Government Support (NISC Guideline and METI's Support)
2. Release of the ISM benchmark in August 2005 and the release of new version of the ISM benchmark
3. Promotion (Handbook, Seminar and Articles about the ISM benchmark)

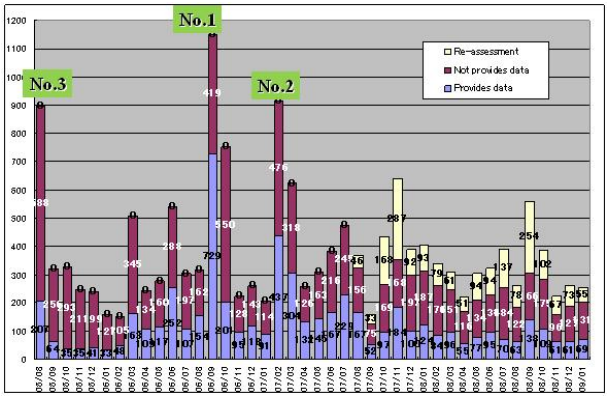


Figure 2-6-6. How well the ISM benchmark is being used (by month)

The ISM benchmark is a comparative and quantitative assessment tool whose assessment results are presented in scores and charts, allowing you to check your organization's position in relation to that of other organizations. In the comparative assessment, the result may change depending on the data with which the user company's data is compared. Considering rapidly changing information security environment, the ISM benchmark version 3.1, which was released on April 21, 2008, was designed to use the data of the past

[15] This can be downloaded from http://www.ipa.go.jp/security/benchmark/benchmark-katsuyou.html

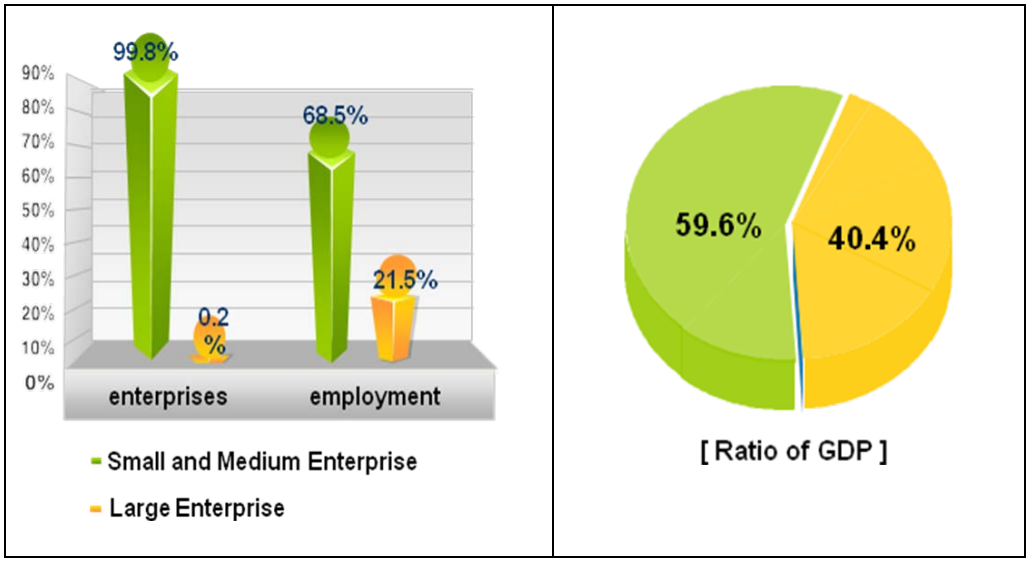
two years as basic data for diagnosis. Statistical[16] information for the basic data has also become available to the public, which helps increase the trust level of users and transparency of the diagnosis.

In this way, with all kinds of efforts, the ISM benchmark was accepted by Japanese users and the number of its users has been increasing.

2.7. Korea

(1) Current Status of Information Security in Business Sector in Korea

An impact of small and medium enterprises (SMEs) in Korea has an important role: 99.8% of domestic enterprises, 86.5% of domestic employment, and 59.6% of gross domestic product (GDP).

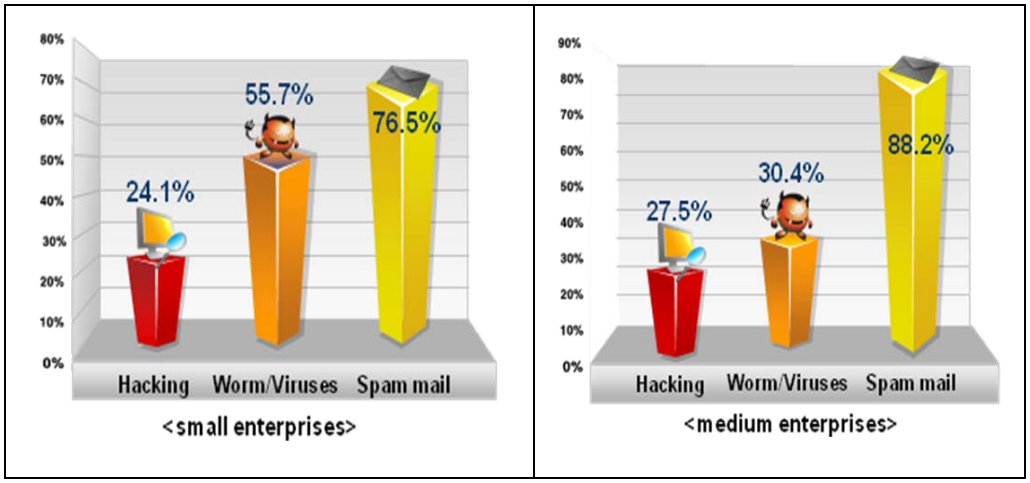


Source: National Statistical Office, and the Small and Medium Business Administration

Figure 2-7-1 Impact of SMEs in Korea

Security Status of SMEs: Over one out of every four SMEs has experienced a security incident. More detailed data on hacking, worm/viruses, and spam mail on small enterprise (1 to 50 employees) and medium enterprise (51 to 300 employees) are illustrated as follows:

[16] You can find the statistic data at http://www.ipa.go.jp/security/english/benchmark_system.html



Source: KISA, Small: 1~50, Medium: 51~300

Figure 2-7-2 Security Experiences of SMEs in Korea

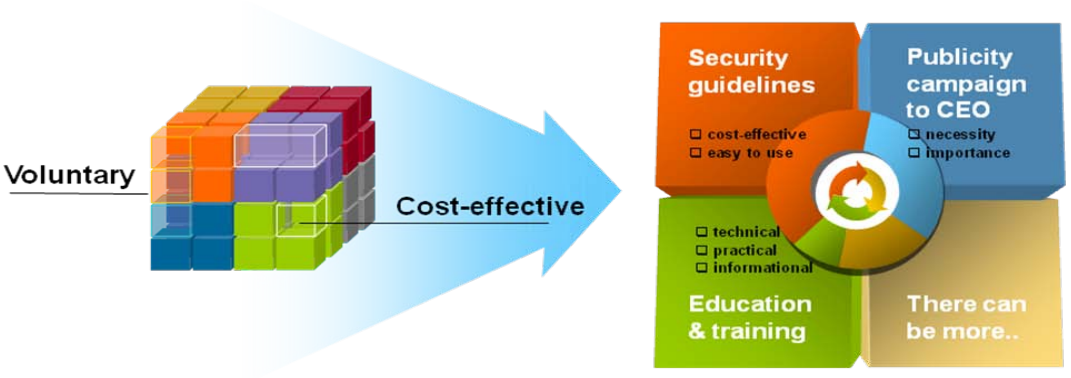
A Cost of security incident by KISA on 10 to 50 employments is summarized:

- Average system recovery time: 10.0 hours
- Average system recovery cost: $14,560

Although the cost of a security incident is very high, a ratio of security investment to the total IT budget is only 2.2% for small enterprises and 6.1% for medium enterprises. The major obstacles why low investment of security is high cost, competency, and difficulty in managing security product.

(2) Government Policies Related to the Business Sector

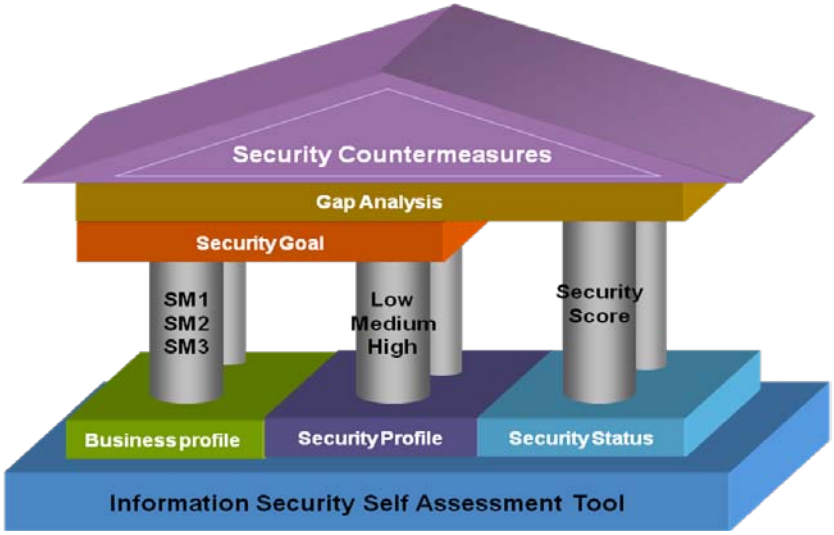
In order to overcome the problem, new action plans on security guidelines and self-assessment tool are introduced by the government. The aim is to enhance the security level of SME with voluntary and cost effective security measures. Security awareness, security goals, and easy to use guidelines are three major factors. The concepts of direction are illustrated as follows:



Source: KISA

Figure 2-7-3 Direction of Action Plans for Security Level Improvement

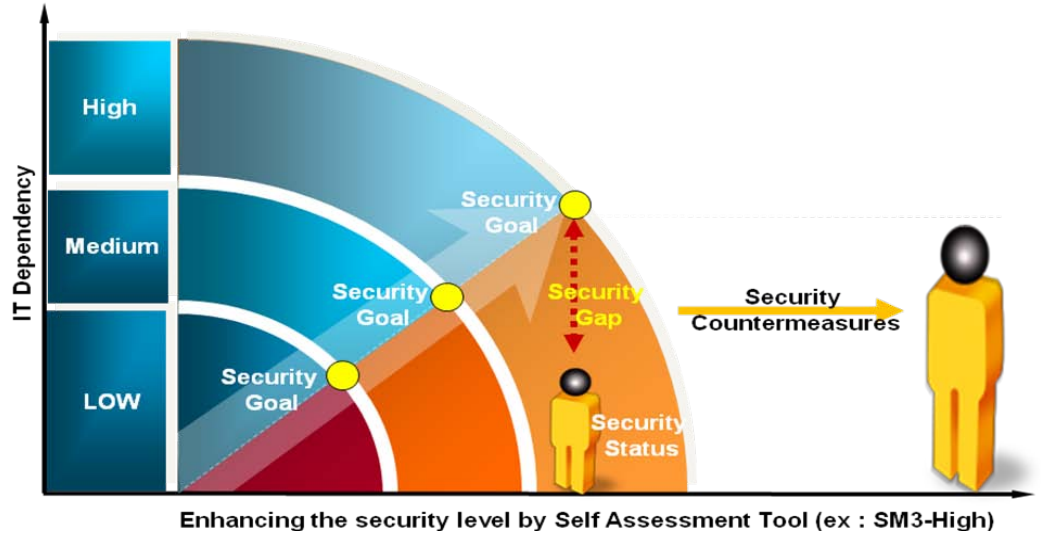
Security guidelines take into account the security requirements for each component of IT infrastructure type, security levels, and assets. Overall architecture for information security self-assessment tool is shown in Figure 2-7-4. The business profile has two components: general information such as total sales employment and IT configuration such as servers, networks, etc. The business profile defines the IT infrastructure type denoted SM1, SM2, and SM3. The security profile shows the IT dependency on security incident and denoted low, medium, and high. When a security incident occurs, disaster recovery capacity, business continuity capacity, and maintenance management capacity are measured as low, medium, and high. Measurement of security status is presented with a security score.



Source: KISA

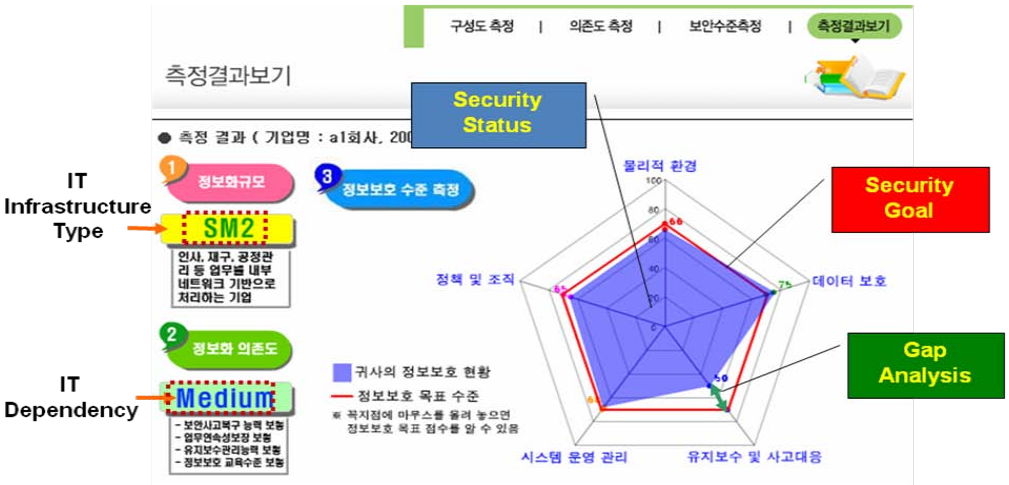
Figure 2-7-4 Architecture of Self-Assessment Tool

Figure 2-7-5 shows a process of gap analysis between security goal and security status. An example of reporting of self-assessment tool is shown in Figure 2-7-6. In the figure, IT infrastructure type, IT dependency, and security status are illustrated item by item. The security goal is also drawn in different colors, and the gap is easily analyzed visually. Also, brief results are summarized by sentences and security countermeasures are reported, too. This self-assessment tool is developed and serviced by the Korea Information Security Agency (KISA).



Source: KISA

Figure 2-7-5 Gap Analysis by Self-Assessment Tool



Source: KISA

Figure 2-7-6 An example of reporting of Self Assessment Tool

(3) Study on Information Security Management Benchmark

i) Selection of companies surveyed

Company selection criteria requested are as follows:

- Domestic companies. Government-linked companies are also acceptable
- A part of global SCM. Specifically, ICT vendor, parts suppliers, EMS (Electronics Manufacturing Service) supplier and other service suppliers are preferred
- Vary in size from SMEs to big companies
- flexibly depending on the each country's situation
- Minimum number of participated Companies: 10

Based on the above criteria, ten Korean companies are chosen:

- Selection of the candidates: Participants among KISA annual awards
- Participated companies (10): Big company-7, SME-3
- Almost all are large companies, some are SMEs. IT & SCM related companies are selected.

ii) Selection of respondents

Requested: referred profiles of the respondents

- -Individuals or groups.
- -Understanding the ISM benchmark.
- -Information security officer

To accomplish the above requests, we consider the following steps:

- -In order to develop the understanding of each participant, we translated the questionnaire for a respondent into Korean and provided an explanation of the ISM benchmark for each company
- Responses are gathered from Chief Security Office's bureau
- Same survey sheets are used

Among the ten companies, we requested analysis result reports from the ISM benchmark. In the Korean case, almost all of the results show very good results (above average level), and some companies show an almost ideal case. Figure 2-7-7 illustrates the result of the participated company. This company shows an ideal security level and higher than average in all fields. Also,

T-score is also with one standard deviation value.

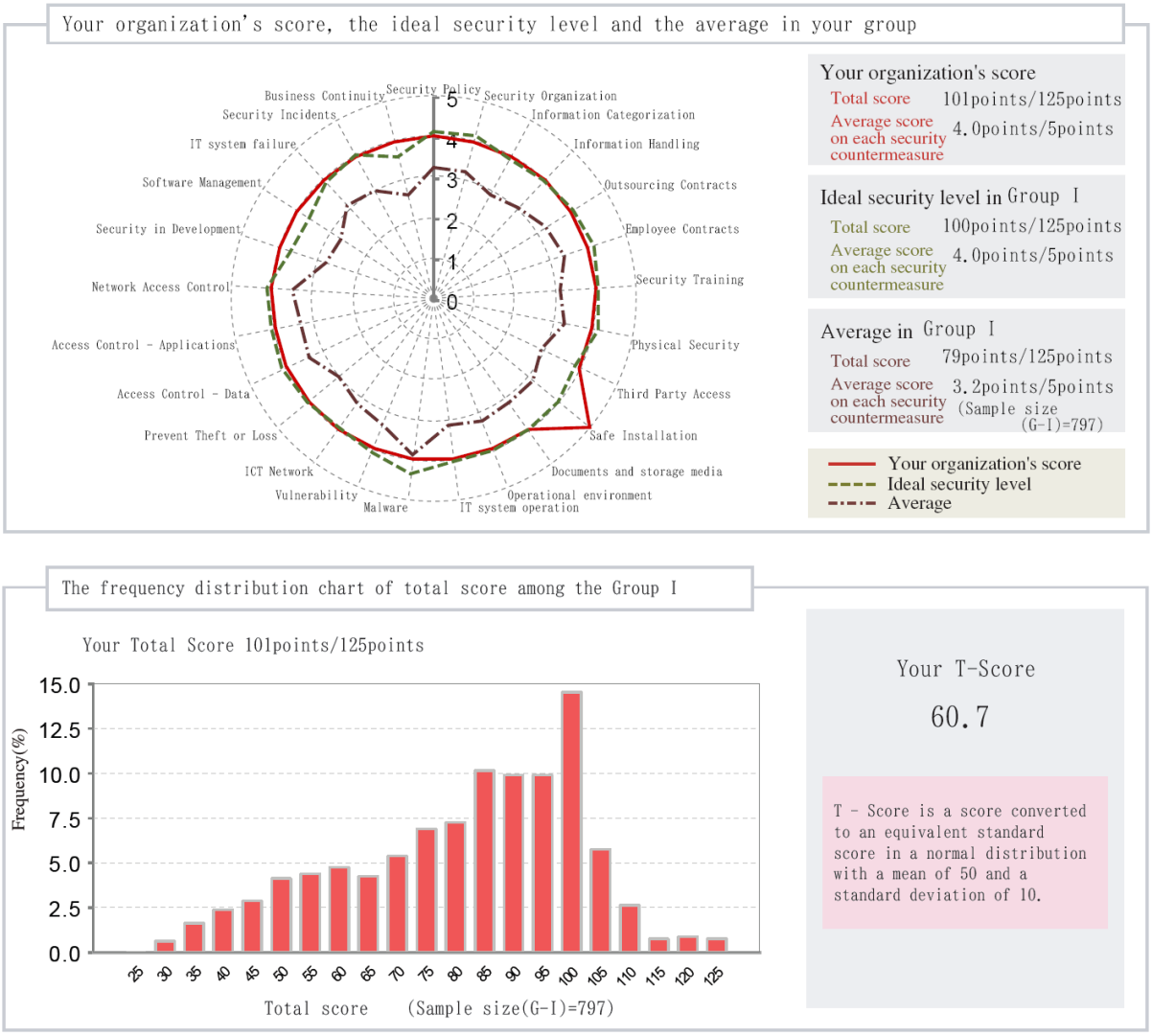


Figure 2-7-7 Example of Korean respondent's ISM benchmark

iii) Analysis of results

Q1. Is the ISM benchmark effective in assessing your company's information security level? (Single Answer):

Sixty percent of respondents answered yes. The reasons were fast response on self-diagnostic and general measure but not in detailed measure. Forty percent answered no. The reasons were weakness on self-diagnostic, no detailed items, and more questions were needed, as well as no objective measure.

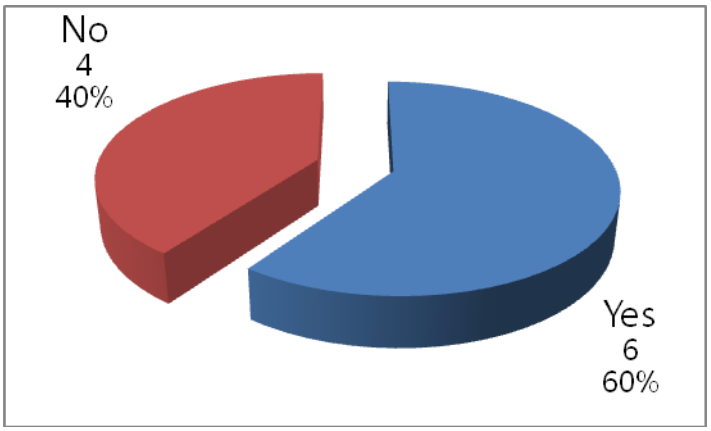


Figure 2-7-8 Effectiveness of Benchmark

Q1-1. If you answered Yes to Q1, in what way do you think that ISM benchmark is effective? (Multiple Choices):

a. To understand the problem domain related to information security.

b. For clues to information security measures.

c. Comparison of the information security level with the average.

Answers for a, b, and c were equally distributed (two of each).

Q2. Are you willing to use the ISM benchmark in your company? (Single Answer):

A majority of respondents did not want to use the ISM benchmarks. The reasons were as follows: Self-measuring tool/checklist was already used, not much flexibility, no objective measure. Some Yes group's reasons for use were possible referencing. Level comparison between the same fields was possible. Guideline for improvement was required. Fast response on security management was possible.

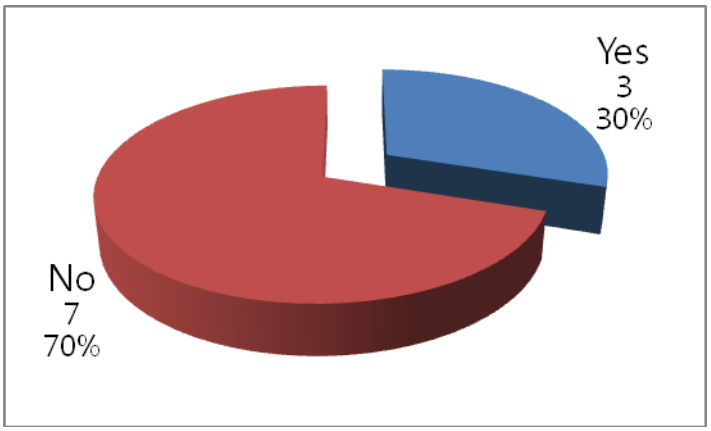


Figure 2-7-9 Willingness to Use

Q2-1. If you answered Yes to Q2, for what purpose do you want to use the ISM benchmark? (Multiple Choices):

a. To check your company's information security level.

c. To report your company's information security level to the clients.

Three answers for a, and one answer in c.

Q3. Is the ISM benchmark easy to use? (Single Answer):

Sixty percent of respondents answered yes. Forty percent responded no. It depended on the respondents. We cannot easily distinguish ease of use.

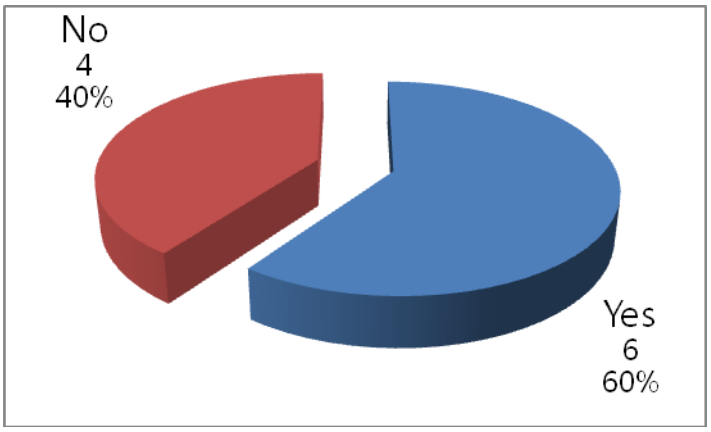


Figure 2-7-10 Ease of Use

Q3-1. If you answered No to Q3, which questions were difficult to answer? (Optional):

Part 2. Option selection on items was ambiguous (not clearly defined).

Q4. Do you have any ideas about additional functions or improvements for the ISM benchmark? (Single Answer):

More than half answered yes and suggested functions to be added summarized in two categories:

a. For questionnaire:

   Detailed measure items on physical/technical/management were required. Reference for option selection was defined clearly. Addition of Security risk on IT project was needed.

b. For result output:

   Option selection on items was ambiguous (not clearly defined). More

items for detail measure were required. Addition of best practice examples in each filed was required.

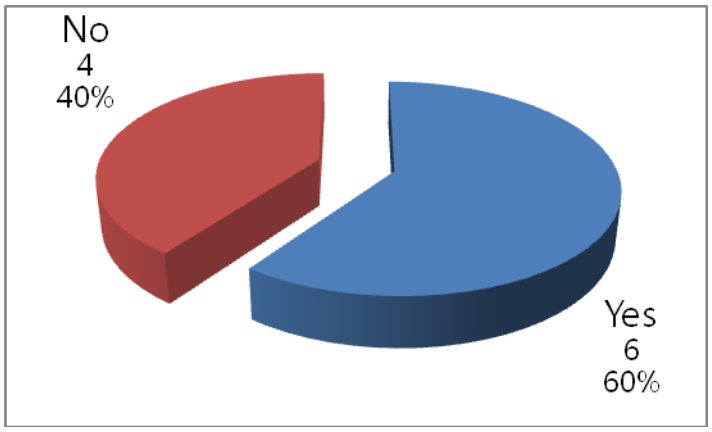


Figure 2-7-11 Additional Functions

Q5. Has your company ever had requests for implementation of information security measures from business partners? (Single Answer, Optional):
More than half answered no because there were no requests from partners.

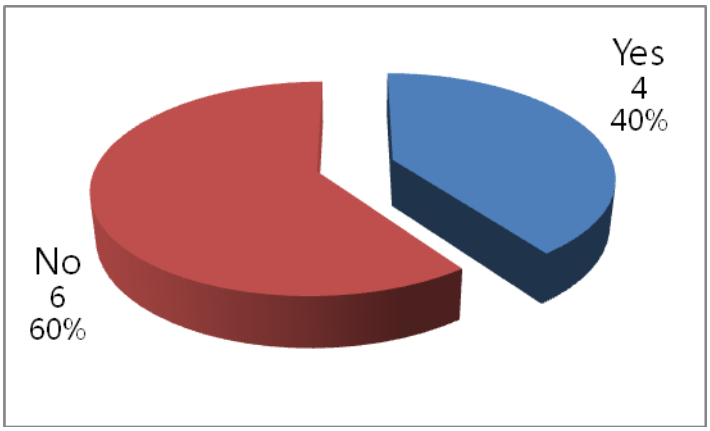


Figure 2-7-12 Information Security Measure Requests from Partners

Q5-1. If you answered Yes to Q5, which standard has your company been requested to comply with from business partners? (Specify):
Internal reference, ISO 27001/27002.

Q6. Has your company ever been requested to implement information security measures by business partners? (Single Answer, Optional):
Almost all respondents answered no. It means that there were not so many requests for such benchmarks from partners. Instead, frequently accredited software was requested during the development of a system. Many security

systems were already in use.

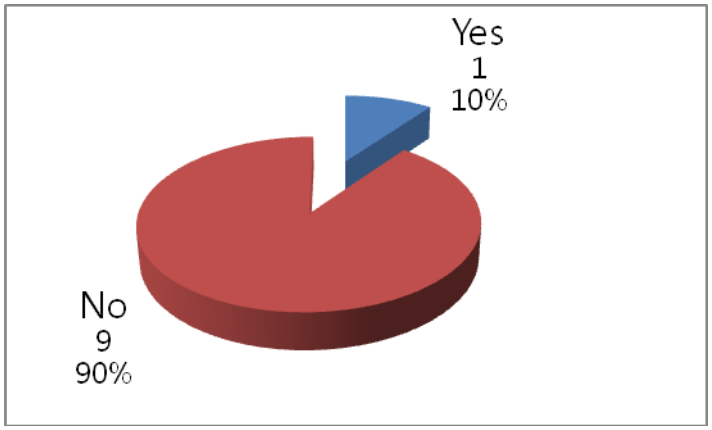


Figure 2-7-13 Information Security Measure Requests to Partners

Q6-1. If you answered Yes to Q6, which standards did your company ask business partners to follow? (Free answer):
Third party measurement on security level was used.

(4) Need for Common ISM benchmark

i) Needs toward Common ISM benchmark

From the results of the survey, Korean companies were divided into two parts. Many of them felt the need for more detailed items and clear explanations of each selection option. This survey may not be at the same level as used in Korea. Thus, examination of benchmarking method proposed by KISA is better to improve ISM benchmarking.

ii) Expected Function to Common ISM benchmark

Many comments from Korean companies required additional items and clear explanation of selection references for detailed measure of security level. Thus, comparison with the Korean security measure survey was necessary.

iii) Roles of Common ISM benchmark

Addition of items for detailed level of measurement is mainly reported. So, some modification of current benchmarking method is better to expand foreign countries (different levels of measure is one possible solution).

iv) Issues

Multiple or level approach may be considered before expansion to foreign countries

For example, a benchmark methods proposed by KISA and Taiwan may be a solution for the common ISM benchmark. Addition of more detailed measure items is requested.

3. Toward Establishment of a Common ISM Benchmark in Asia

3.1. Notice of Interpretation Regarding the Survey Results

We conducted a survey on the trial use of the ISM benchmark in order to consider the needs and requirements for the Common ISM benchmark. Specifically, we asked several companies, who were ERIA WG members, excluding Japan, and who had created the ISM benchmark, to use the ISM benchmark and analyzed the results.

We received answers from 48 companies in total in the member countries (six countries). Table 3-3-1 shows the breakdown of the answers.

Table 3-3-1 Attributes of respondents

	Total	Size		Type of Industry
		Large	SMB	
Malaysia	13	54%	46%	NA
Singapore	4	0%	100%	NA
Thailand	3	67%	33%	Internet provider, healthcare, agriculture organization
Vietnam	14	43%	57%	Information service, manufacturing, telecom, finance/insurance, broadcasting, publishing/newspaper, public welfare
China	6	50%	50%	Information service, software evaluating and testing, credit card manufacturing, information security product developing, internet gaming, HR service for foreign company.
Japan	NA	NA	NA	
Korea	10	70%	30%	Medium-sized companies, some SMEs, IT, and SCM related companies

The ratio of respondent small/mid-sized and large companies is relatively balanced. Many of the companies are in IT-related, information services, other services, and manufacturing industries. For the following reasons, we must keep in mind that the results of this survey may not reflect the conditions of the countries above correctly:

- Each WG member had its own sampling method.
- The number of samples was small.
- The person in charge of information security from each company did not answer the survey questions as the representative of the company.
- We did not ask respondents to give details on security measures.

From the sampling problem, the analysis of the survey results had statistical limits on accuracy. In addition, because the person in charge of information security from each company did not answer the survey questions as the representative of the company, it is appropriate to consider the diagnostic results from each ISM benchmark as a guide. However, the opinions on the ISM benchmark from these companies are reliable.

3.2. Analysis of the Needs for the Common ISM Benchmark

We gathered opinions on the effectiveness and use of the ISM benchmark from participating companies in the member countries in order to research the need for the Common ISM benchmark. Up to 60% to 100% of the companies surveyed answered that they considered the ISM benchmark effective in assessing their information security levels (see Table 3-3-2).

From the table above, we can see that the effectiveness of the assessment of each company's security level using the ISM benchmark was relatively highly evaluated. Looking closely at the table above, evaluations by Korea was lower than those of the other counterparts, which may be attributed to the following:

- Korean companies experienced progress in IT, which created more sophisticated needs for information security.
- Korea has an existing benchmark.
- Korea have different industrial structures compared to those of the other counterparts.

Table 3-3-2 Is the ISM benchmark effective in assessing your company's information security level?

	Yes	No	Comment
Malaysia	83%	17%	- It is effective for high level assessment.
Singapore	67%	33%	- Fairly comprehensive; it is able to provide an answer to the question asked; - All of the above provided answer. - Current approach appeared to be at a level that was too high, which essentially only answered the question as to whether an ISMS was in place. - Unlikely to see significant changes in the survey results once ISMS has been implemented. - Lack of ISMS itself cannot be the justification for implementing the ISM benchmark.
Thailand	100%	0%	- Very useful, effective in assessing the organization's IT security level
Vietnam	100%	0%	- A lot of information on information security can be obtained. - Practical and easy-to-use.
China	100%	0%	NA
Japan	NA	NA	NA
Korea	60%	40%	- Fast response for the self-diagnostic section. General measure but not in detailed measure. - Weakness on self-diagnostic section. No detailed items, more questions are needed. No objective measure.

Then, when we asked in what way was the ISM benchmark effective, we obtained the following responses: "To know your problems related to information security," "To obtain advice about information security measures," and "To compare the information security level with the average.". These answers were at almost the same ratio.

From 30% to 93% of the respondents answered that they wanted to use the ISM benchmark (see Table 3-3-3). Seeing the trend, the ratio of answers is similar to that of the effectiveness of the security level assessment (see Table

3-3-2). However, companies in Korea want to use the benchmark less. The reasons for this seem to be the same as explained above.

Table 3-3-3 Are you willing to use the ISM benchmark in your company?

	Yes	No	Reason (Comments)
Malaysia	86%	14%	Yes: It is an effective tool. No: Have own standard i.e. Cobit + homegrown standard.
Singapore	67%	33%	Yes: - It needs improvements in reducing repetitive questions, easier to understand questions in terms of its grammar and construction and the way it is structured. - To check your company's information security level No: - Concern over misuse and breaches of survey data, require higher management approval and support.
Thailand	NA	NA	- Some respondents are willing to use the ISM benchmark to check the company's security level.
Vietnam	93%	7%	Yes: Free and easy-to-use. Effective tool for assessing the information security level. We can see improvements in information security through this benchmark.
China	83%	17%	No: The ISM benchmark is too general, a more specific benchmark suitable to our company is needed.
Japan	NA	NA	
Korea	30%	70%	Yes: Possible referencing. Level comparison between the same fields is possible. Guidelines for improvement are required. Fast response to security management is possible. No: Self measuring tool/checklist is already used. Not so much flexibility. No objective measure.

3.3. Analysis of Functions Required for the Common ISM Benchmark

In order to research the functions for the Common ISM benchmark, we gathered opinions from companies in the participating countries on usability and the added functions of the ISM benchmark.

From 60% to 100% of the respondents answered that the benchmark was usable. The respondents rated the benchmark highly for the following reasons:

- The results are graphically and clearly displayed.
- Easy-to-use because diagnosis on the Web is available.
- Great because tips and hints are displayed with the diagnostic results.

Meanwhile, we received the following opinions:

- Difficulty: Too difficult for beginners.
- Relationship with other standards: Relationship with ISO/IEC 2700x is unclear.
- User interface: Difficult to understand how the assessment results are output.
- Operational instability: The system does not work properly in some environments.
- Problems with questions: Unclear definitions and meanings, redundant questions. There is room for improvement in the question structure.
- Problems with alternatives: “Not applicable” should be added.
- Other: Commercially available? Who owns the copyright on the results?

We received the following opinions on the added functions and improvements for existing functions:

- Supported languages: Other languages should be supported in addition to English.
- Support for local servers: Installing the benchmark system in each country
- Questions: More detailed questions should be added. (E.g., technological measures for FW etc., human resources and IT security risks etc.)
- Customization: Questions can be added by different countries and companies.
- Understandability: More detailed explanations on the diagnostic results, best practices in each field, and guidelines should be added.

3.4. Common ISM Benchmark in Expansion of Direct Investment and Outsourcing in Asia

We asked the participating companies whether they had been asked for information security measures by their business partners or had requested information security measures of their business partners in order to analyze the need for the Common ISM benchmark especially from the perspective of expansion of direct investment and outsourcing (see Table 3-3-4).

From 29% to 50% of the companies answered that they had been asked for information security measures by their business partners. From 10% to 36% answered they had requested information security measures of their business partners. Specifically, they had been asked or had requested compliance with ISO/IEC 2700x, PCI-DSS, proprietary standards, installation of VPN, SSE-CMM, and third-party evaluations.

Table 3-3-4 Information security measures requested by/of business partners

	Requested by business partners		Requested of business partners	
	Yes	No	Yes	No
Malaysia	29%	50%	14%	72%
Singapore	67%	33%	33%	67%
Thailand	NA	NA	NA	NA
Vietnam	50%	50%	36%	64%
China	33%	67%	17%	83%
Japan[17]	63%	28%	56%	42%
Korea	40%	60%	10%	90%

From the results shown above, information security measures have become more important in business relations in Asian countries. Therefore, the Common ISM benchmark to more easily check the information security levels of business partners is needed for expansion of direct investment and outsourcing.

[17] The percentage for Japan comes from the "Actual Condition Survey on Methods to Check Information Security Measures of Small-and-Medium-Size Companies" conducted by the IPA, not from this survey. http://www.ipa.go.jp/security/fy19/reports/sme/index.html

Meanwhile, the following problems were identified in using the existing ISM benchmark for such a purpose:

- Generic nature of the questions does not provide sufficient information to differentiate the security strength of companies involved
- Few SME and local companies would achieve 4 and even less would achieve 5

Current needs focus on a specific certification plan related to each regulation/standards required.

3.5. Toward Establishing the Common ISM Benchmark in Asia

Based on the results of the analysis, we agreed to offer the following vision and goals as WG1:

Our Vision:
A common ISM benchmark contributes to industries and governments by building and promoting a trustworthy economic partnership that encourages more foreign direct investment (FDI) and business outsourcing in the Asian region.

Goals:
- The common ISM benchmark provides acceptable and comparable indicators of the information security management level of organizations.
- As a comprehensive risk communication tool, the common ISM benchmark enables organizations to improve their sense of information security through visualization of the risks.

In order to achieve the vision and goals above, we must overcome the challenges to implementing the common ISM benchmark. We must consider these challenges in the future.

(1) Positioning of the common ISM benchmark

- What type of company should be targeted (large or SMB)?

(2) Specification of the common ISM benchmark

- How the questions (assessment items to be asked) should be?
- How the assessment criteria should be?
- How the assessment result should be?

(3) Customization and Localization

- How the localization of each country should be?
- To what extent should customization be permitted in each country?
- Is the localization only the language issue?
- How should we ensure compatibility and comparability among versions for different countries when permitting these countries to customize the benchmark?

(4) Operational Framework

- Who will manage and operate the common ISM benchmark?
- How we should consider the local server and local operation?
- In the relationship of above 2 questions, how the collected data should be treated, it should be treated in each nation separately or do we need centralized server and centralized data analysis?

IV. Conclusion

In this research, we studied the development of the common information security management benchmark (common ISM benchmark) in the Asian region.

First, we analyzed how the establishment of information security would impact the Asian economy or enterprise management in Asia and studied the role that the common ISM benchmark plays in the region. For this purpose, we pointed out that risk management involved with collaboration among companies is required in order to develop closer collaboration in the Asian region and to promote foreign direct investment (FDI). We showed that the establishment of information security management in the value chain was an essential element of this risk management. We also showed that the common ISM benchmark could support information security management in the value chain by providing a common method for companies to easily evaluate their information security levels in comparison with one another (III-1).

We then studied the conditions and challenges to enterprise information security measures in the Asian region. In addition, we conducted a survey on the trial use of the ISM benchmark in order to consider the needs and requirements for the Common ISM benchmark. Specifically, we asked several companies, who were ERIA WG members, excluding Japan, and who had created the ISM benchmark, to use the ISM benchmark and analyzed the results. We received answers from 48 companies in total in the member countries (six countries). Table 1 shows the breakdown of the answers.

Through trial use, the majority of the companies approved the ISM benchmark as an effective tool in evaluating the enterprise information security level; we generally obtained a positive result for the development of the common ISM benchmark. Meanwhile, we found that it was difficult to cover all cases with the ISM benchmark (III-2) alone.

Finally, WG achieved the following settlement after we considered our vision and goals based on these results (III-3):

Our Vision: A common ISM benchmark contributes to industries and governments by building and promoting a trustworthy economic partnership that encourages more foreign direct investment (FDI) and business outsourcing in the Asian region.

Goals: - The common ISM benchmark provides acceptable and comparable indicators of

the information security management level of organizations.
- As a comprehensive risk communication tool, the common ISM benchmark enables organizations to improve their sense of information security through visualization of the risks.

Some problems have yet to be resolved to establish the common ISM benchmark in the future. These problems are shown below:

(1) Positioning of the common ISM benchmark

- What type of company should be targeted (large or SMB)?
- Should only Asian countries or the entire world be targeted?

(2) Requirements for the common ISM benchmark

- To what extent should customization be permitted in each country?
- How should we support each language (localization)?
- Should several assessment criteria be established as opposed to only one assessment criterion?

(3) System under which the common ISM benchmark is established and operated

- How do we ensure human resources with the necessary expertise to establish the common ISM benchmark and a system that enables collaboration with other standards groups?
- Who manages data collected through the common ISM benchmark and systems, and who analyzes the data?
- How should we ensure compatibility and comparability among versions for different countries when permitting these countries to customize the benchmark?

These problems are difficult to resolve but taking the first step toward establishing information security management in the value chain is inevitable. In addition, consolidating the development of Asia requires constructing a more advanced cross-border common infrastructure suitable for a knowledge-based economy and appropriate for the knowledge-based economy era. As part of this effort, it is important

to place enterprise information security as a strategic policy in the region. From the perspective of establishing a new collaborative model in the Asian region, it is important for Asia, which has an important role in the world economy, to take the initiative in developing this common ISM benchmark.

This policy research is the first trial led by the Asian region as well as for the ERIA. However, we think we have successfully obtained substantial results from this policy research. It is important to continue efforts towards the realization of a common information security infrastructure in Asia based on the results of this research for the development of the region.

V. Appendix 1. Member List

Leader

<Thailand>

- Dr. Komain Pibulyarojana, Director of Programmes for Information Technology for National Security, ThaiCERT, National Electronics and Computer Technology Center (NECTEC)

Member

<China>

- Mr. Wang Xin Jie, CEO, Beijing Powertime Co., Ltd.

<Japan>

- Mr. Eijiroh Ohki, Professor, Kogakuin University, Japan
- Dr. Suguru Yamaguchi, Professor, Nara Institute of Science and Technology

<Korea>

- Dr. Young Bin Kwon, Professor, Chung-Ang University

<Malaysia>

- Mr. Mohamad Shamir Bin Hashim, Head of Division, Strategic Policy & Cyber Media Research, CyberSecurity Malaysia

<Singapore>

- Dr. Meng Chow Kang, Co-chair, RAISE Forum, Singapore

<Vietnam>

- Dr. Hoang Dang Hai, Deputy Director General, Vietnam Computer Emergency Response Team (VNCERT)

Consultant

<Japan>

- Ms. Yasuko Kanno, Chief Advisor, IT Security Center (ISEC), Information-Technology Promotion Agency (IPA)
- Mr. Masayasu Murano, Senior Research Professional, Mitsubishi Research Institute (MRI)
- Mr. Shuji Kawaguchi, Chief Research Professional, Mitsubishi Research Institute (MRI)
- Ms. Kaori Maruta, Research Professional, Mitsubishi, Research Institute (MRI)

Observer

<Japan>

- Dr. Ikuo Misumi, Director, Office of Information-Technology Security Policy, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
- Mr. Kazushi Izuchi, Deputy Director, Office of Information-Technology Security Policy, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
- Mr. Tomoharu Shimizu, Deputy Director, Office of Information-Technology Security Policy, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
- Mr. Hiroaki Wada, Office of Information-Technology Security Policy, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
- Dr. Ayumi Kodama, Assistant Director, Information Policy Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
- Mr. Masayuki Ogata, Deputy Counselor, National Information Security Center(NISC), Cabinet Secretariat
- Mr. Toshihiko Suguri, Deputy Counselor, National Information Security Center(NISC), Cabinet Secretariat
- Mr. Yujin Kume, National Information Security Center(NISC), Cabinet Secretariat
- Mr. Kunitaka Hashizume, Executive Director, Center of the International Cooperation for Computerization (CICC)

Coordinator

<Japan>

- Mr. Yutaka Ikeda, General Manager, Center of the International Cooperation for Computerization (CICC)
- Ms. Hiroko Kawabata, Center of the International Cooperation for Computerization (CICC)
- Ms. Kaori Umemura, Center of the International Cooperation for Computerization (CICC)
- Ms. Tomoko Asai, Center of the International Cooperation for Computerization (CICC)

VI. Appendix 2. IPA Information Security Management Benchmark (ISM benchmark)

1. Overview

The ISM Benchmark is a self-assessment tool to visually check where the level of the user company's security measures resides by responding questions about company profile and 25 items of security measures. IPA developed the web-based self-assessment tool based on the concept of METI and released the system on the IPA's web site in August 2005.

For the ISM Benchmark, user companies (or user organizations) are classified into three groups (see Table A2-1), based on the Information Security Risk Index (hereafter referred to as "Risk Index"). Risk Index indicates risks to which organization is being exposed. Risk Index is calculated based on several factors, including the number of employees, sales figures, the number of critical information held and so on. Categorizing organizations into three groups supports organizations in establishing information security measures based on their level (high, medium, or low) and determining reasonable security expenses.

Table A2-1 Classification According to Risk Index

Type	Characteristics
Group I	High level IT security measures are required
Group II	Medium level IT security measures are required
Group III	Not thorough IT security measures are required

To conduct diagnosis, the ISM Benchmark requires users to answer questions on its Website. Part I consists of 25 questions regarding information security countermeasures and Part II contains 15 questions about corporate profile. When the 40 questions are answered, diagnostic outcome and recommended approaches are displayed.

As a diagnosis outcome, the following items are displayed (see Figure A2-1):

(1) A scatter chart that shows the company's position in the group;
(2) A radar chart that shows implementation status of 25 security measures;
(3) Scores for the 25 questions.

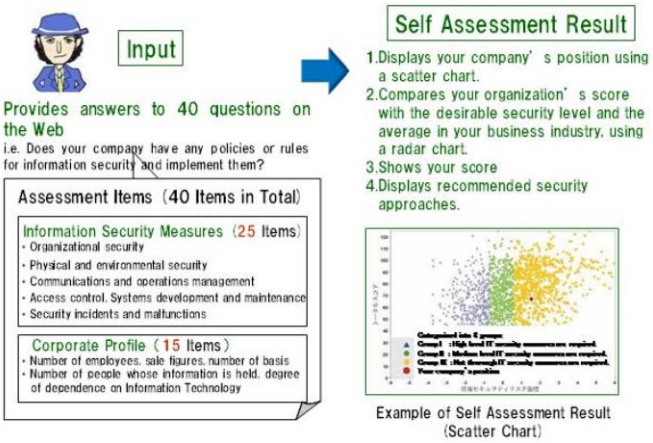


Figure A2-1 Input and Output of ISM Benchmark

2. Questions

Regardless of group, all the organizations to be diagnosed need to answer 25 information-security-related questions (see Table A2-2) on the following one-to-five scale: (1) No policy or rule has been established (2) Only some part of it is implemented (3) Implemented but the state has not been reviewed (4) Implemented and the state reviewed on a regular basis (5) Implemented enough to be recognized as a good example for others. The highest score is 125 points with each question giving 5 points at best.

Table A2-2 ISM Benchmark List of Evaluation Items

1. Information Security Policy
2. Security Organization
3. Categorization of Information Assets
4. Handling of Information Assets
5. Outsourcing Contracts
6. Employee Contracts
7. Security Training
8. Physical Security
9. The Third Party Access
10. Safe Installation
11. Documents and storage media
12. Security in operational environment
13. Security for IT system operation
14. Countermeasures against Malware
15. Measures for Vulnerability
16. Measures for Communication Networks
17. Prevent Theft or Loss of Media
18. Access Control - Data
19. Access Control - Applications
20. Network Access Control
21. Security in System Development
22. Security Management of Software
23. Measures for IT system failure
24. Incidents Handling
25. Business Continuity Management

3. Assessment Result

Using assessment result, users can check their organization's score and compare it with that of other organizations. For comparison, a radar chart and a scatter chart are displayed to allow users to check where the level of the organization resides. The basis of these comparisons is diagnosis data that was collected through the self-assessments performed by other organizations using the ISM Benchmark.

Self-assessment results contain the following items:

a. Scatter Chart – shows the distribution of all the companies and the organization's position.

- Presents two types of distribution: all (in three groups) or organization-size-based.
- Compare the organization's position with other companies.
- Compare the organization's current position with past two positions.

b. Radar Chart –compare a score with that of others from four different angles.

- Group-based Comparison − compare a score with that of others in the same group which is classified based on the information risk index.
- Organization-size-based Comparison - compare a score with that of others in the same group which is classified based on the size of the organization.
- Industry-based Comparison - compare a score with that of others in the same group, which is classified based on the business industry.
- Time series Comparison - compare organization's current position with past two positions.

c. Frequency Distribution and T-score of Total Score.

d. Self-Assessment Results in PDF format

e. Score List.

f. Recommended Information Security Approaches.

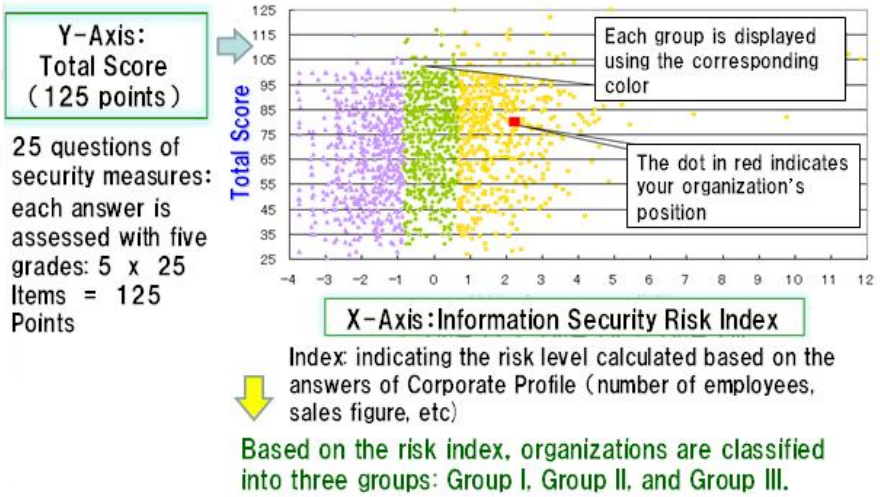


Figure A2-2 Assessment Result (Scatter Chart)

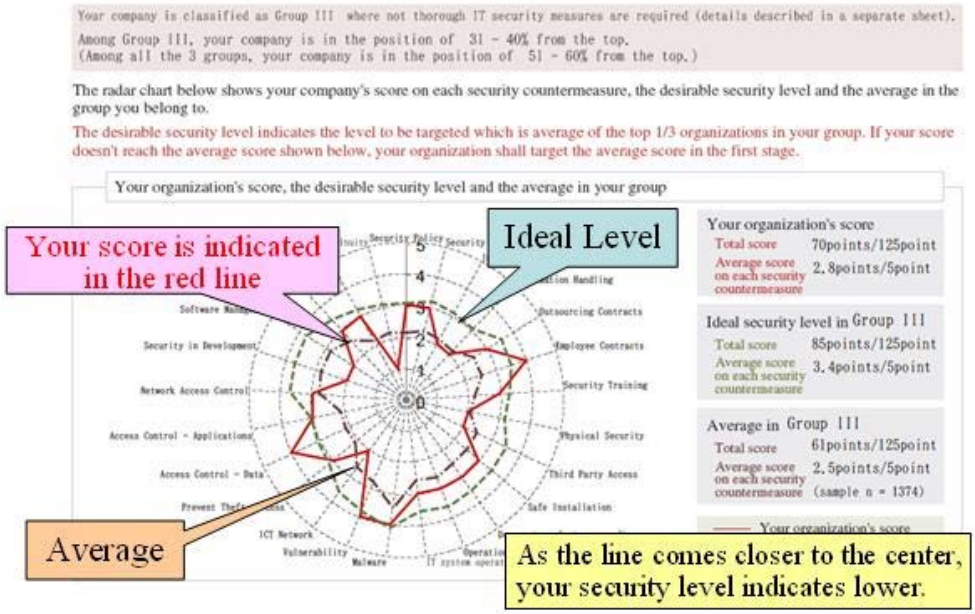


Figure A2-3 Assessment Result (Radar Chart)

4. Usage

Table A2-3 shows the number of records collected from Aug. 4, 2005 to Mar. 19, 2008. By March 19, 2008, the number of records had exceeded 13,000. Among those records, more than 5,000 records (including 885 for initial records) are used by this system as basic data for diagnosis until Mar. 19, 2008.

Table A2-3 Number of Diagnosis Performed (As of Mar. 19, 2008)

Period	Diagnostic Data Provided for the System (Total Number)	Diagnostic Data Not Provide for the System (Total Number)	Total (Total Number)
Initial Data (March 2005)	885*	—	885
Ver. 1.0 (Aug. 4, 2005 to Mar. 19, 2006)	490	2008	2498
Ver. 2.0 (Mar. 20, 2006 to Dec. 17, 2007)	4062	4689	8751
Ver. 3.0 (Dec. 18, 2007 to Mar. 19, 2008)	325	604	929
Total	5762	7301	13063

* Initial data (885) was collected from a questionnaire that was conducted at the time this system was developed.

VII. Appendix 3. Questionnaire for Respondents

Q1. Is the ISM benchmark effective in assessing your company's information security level? (Single Answer): Yes / No

Reason (specify):

Q1-1. If you answered Yes to Q1, in what way do you think that ISM benchmark is effective? (Multiple Choice):

a. To understand the problem domain related to information security.

b. For clues to information security measures.

c. Comparison of the information security level with the average.

d. Other ( ).

Q2. Are you willing to use the ISM benchmark in your company? (Single Answer): Yes / No

Reason (specify):

Q2-1. If you answered Yes to Q2, for what purpose do you want to use the ISM benchmark? (Multiple Choice):

a. To check the company's information security level.

b. To check the supplier's information security level.

c. To report the company's information security level to clients.

d. Other ( ).

Q3. Is the ISM benchmark easy to use? (Single Answer): Yes / No

Q3-1. If you answered No to Q3, which questions were difficult to answer? (Optional):

Q4. Do you have any ideas about additional functions or improvements for the ISM benchmark? (Single Answer): Yes / No

Functions to be added (specify)

a. For the questionnaire:

b. For results output:

Q5. Has your company ever received requests for implementation of information security measures from business partners?

(Single Answer, Optional): Yes / No

Q5-1. If you answered Yes to Q5, which standards has your company been requested to comply with from business partners?

(Specify):

cf. ISO/IEC 27002, PCI-DSS.

Q6. Has your company ever asked business partners to implement information security measures? (Single Answer, Optional): Yes / No

Q6-1. If you answered Yes to Q6, which standards did your company ask business partners to follow?

(Specify):

cf. Original standards of your company, ISO/IEC 27002, etc.

VIII. Appendix 4. List of Authors

List of Authors	
I. Background and Objectives	Dr. Komain Pibulyarojana
II. Overview of the research	Dr. Komain Pibulyarojana
III. Research for strengthening information security in the business sector	
1. Economic impact of strengthening information security in ASEAN and East Asia	Mr. Eijiroh Ohki
2. Current status of information security in business sector	
2.1. Malaysia	Mr. Mohd Shamir Bin Hashim
2.2. Singapore	Dr. Meng Chow Kang
2.3. Thailand	Dr. Komain Pibulyarojana
2.4. Vietnam	Dr. Hoand Dang Hai
2.5. China	Mr. Wang Xin Jie
2.6. Japan	Dr. Suguru Yamaguchi Information on (3) was provided by Ms. Yasuko Kanno
2.7. Korea	Dr. Young Bin Kwon
3. Toward establishing international common benchmark	Mr. Eijiroh Ohki
IV. Conclusion	Dr. Komain Pibulyarojana