Outline
of
AFIT Member Countries/Regions' Data
on
Information Security

AFIT Secretariat

February 19, 2009

Survey Sheet Contents

A. Basic IT Infrastructure Data

(No. of PC/Internet User/IT human resources/fixed telephone/cellurar phone)

B. Related IT Security Data

(Amount of damage due to eCrime/Government budget)

C. Information Security Key Terms to Explain Present Situation of Each Country/Region

1.Organization responsible for national security and critical infrastructures

2.Legal Systems (Legislation)

3.Introduction of standardizaiton, evaluation and certification system

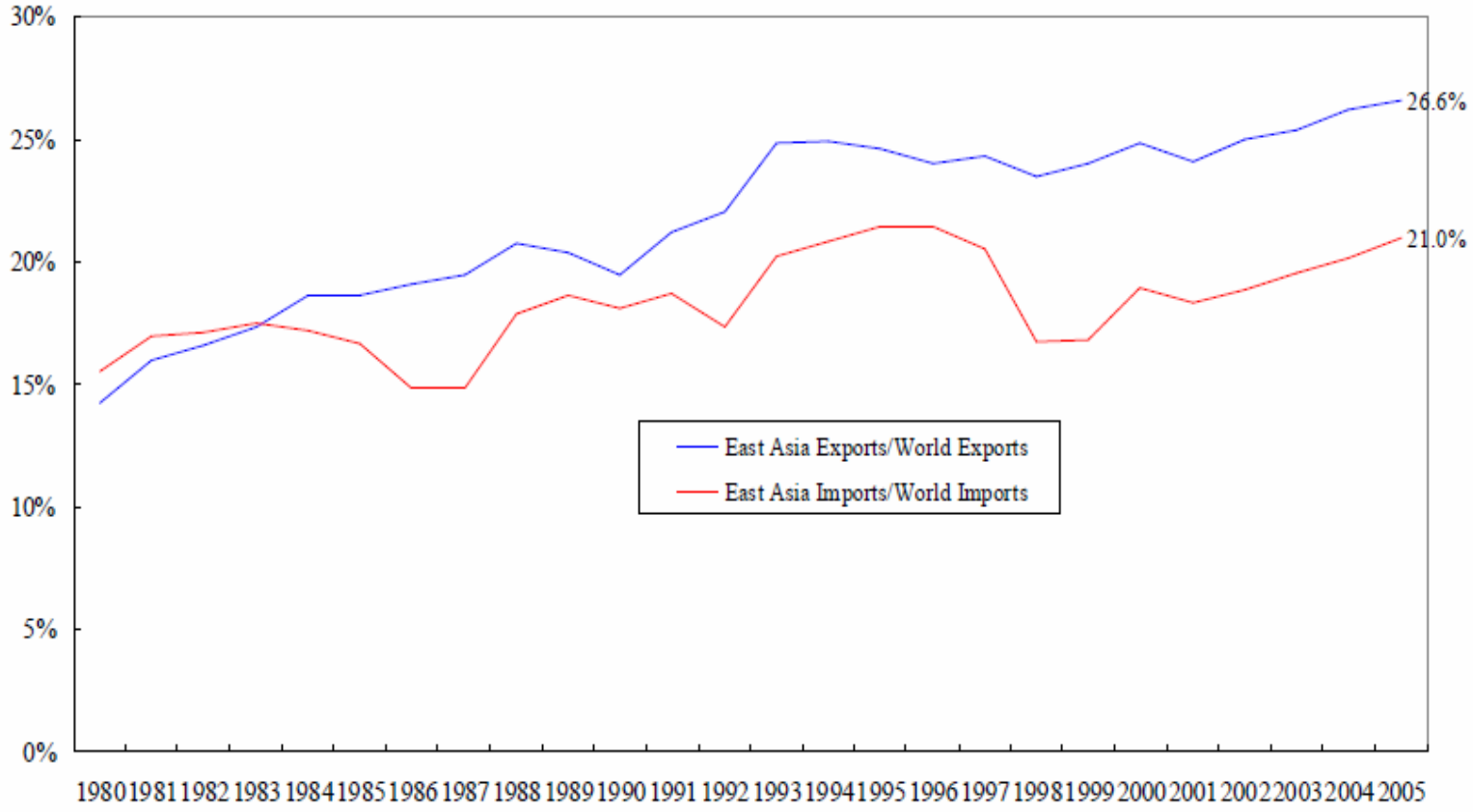
4.Promotion/supportive measures conducted by government

D. Security incidents

From “White Paper on International Economy and Trade 2008”

Asia is keeping vigorous economy.

Figure 2-1-40 Share of Asia in World Trade

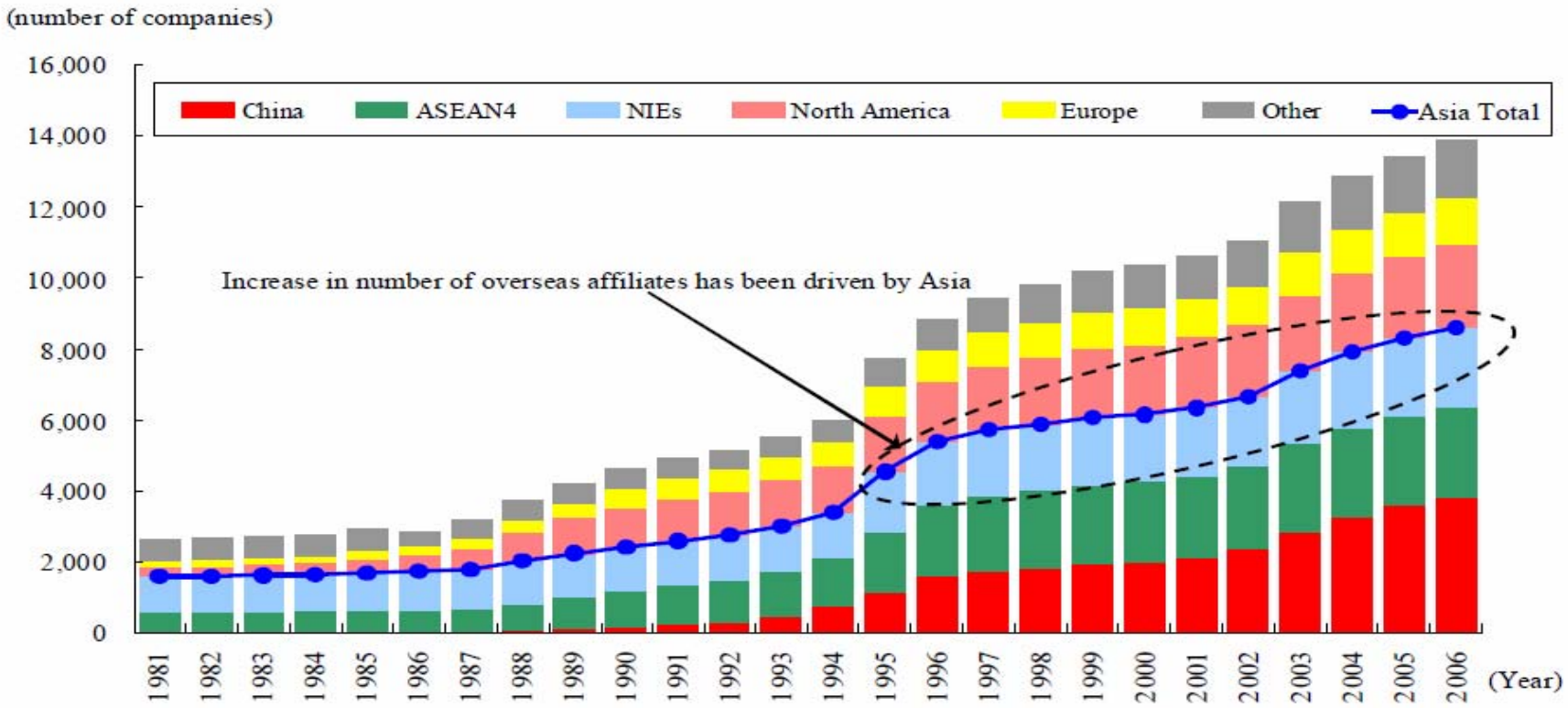


Note: Not including trade in services.

Source: Research Institute of Economy, Trade & Industry, IAA, *RIETI-TID2007*.

From “White Paper on International Economy and Trade 2008”
Growing close tie with Asia

Figure 1-1-22 Changes in the number of overseas affiliates of Japanese manufacturers



Note: Europe includes Russia. "Asia total" refers to the aggregate of: China, ASEAN4, and NIEs.
Source: Annual editions of the Kaigai Shinshutsu Souran [Kunibetsuhen] (Toyo Keizai).

Figure 1-1-23 Changes in the sales, recurring profits, and overseas production ratios (manufacturers) of overseas affiliates of Japanese companies

Incidents:

- Major Sri Lankan manufacturer received scam emails warning that they would lose their domain name registrations. Such domain name registration scams have occurred frequently throughout 2008.

- PNP of Philippines monitored 446 defaced government websites mostly owned local governments in 2006. There were 34 defacement incidents, of which 23 are local government websites.

- There occurred attacks on the bank websites and phishing cases for the banks in Indonesia.

- The websites of government on critical sectors organization are necessarily hosted in India. Private sector are free to host their websites anywhere in the world. Over 800 websites of Indian enterprises hosted in India had their websites defaced in 2008.

- Data leakage incidents occurred in most of the sectors, some government departments and public organizations, commercial companies like banks and local celebrities in Hong Kong.

- In Japan, IPA reported that over the 2008 virus infection mechanism is getting further sophisticated, such as relatively safe PDF file or Word file hide some virus, renowned business or organization's websites are altered for infection, and virus appeared via USB memory.

Tendency of threats (technical, physical and personal) are prevailing from governmental sector to business sector/individual.

SYSTEM PROBLEMS:

- Kuala Lumpur Stock Exchange: In 2008, one of the module in KLSE Stock exchange system was down and decided to switch using back-up system for that module only. Synchronization of data between primary and back-up site takes 3 hours a longer time than anticipated causing KLSE to stop resuming trading in the afternoon.

- Air Lines: In 2008, a glitch in the computer systems of All Nippon Airways Co. Ltd., eventually caused 130 cancellations and delays of more than an hour for 306 flights and around 69,300 passengers were affected. The problem hit data flowing between the airline's main reservations host computer and intermediate computers that handled downstream connections to terminals in airports. The problems began to resolve themselves on Sunday afternoon and by Monday morning the airline was operating close to a normal schedule. In the last two(2) weeks, three of the six intermediate computers that sit between the host and airport check-in terminals were replaced.

Those kinds of system problems (technical and accidental) are also threats to information security. But panel discussion excludes these issues.

Damages:

- In Japan, e-crime damage amount is estimated approx. 2.9 billion US dollars in 2003 using IPA (Information-Technology Promotion Agency) assessment model. This amount is 0.6% of general expenditures. Government budget for information security for 2007 around 0.3 billion US dollars. This amount accounts for 0.06% of general expenditures.

- In Malaysia, it is estimated 0.8 million US dollars (307 cases) cyber crime reported in 2006 by Royal Malaysian Police.

- In India, the government has earmarked 1-3% of annual budget of each Ministry and State for implementation of e-Government applications. It is observed that 15-20% of it is being used or implementing Cyber Security , both for equipment installation and training

Only Malaysia、India and Japan reported damage amount or government budget .

It seems to be important at first stage to recognize the damage/risk in figures for risk management of information security (considering information assets, threats and vulnerabilities) since investment is necessary to prevent the damages, though it is rather difficult to measure the risk.

Organizational fight with threats in each country:

Operation Unit / Policy Making Unit has each history and background in each country/region.

Bangladesh:	Bangladesh Telecom Regulatory Commission	>policy making unit
India:	CERT-IN under Department of Information Technology	>operation unit
Indonesia:	Depkominfo, ID-SIRT and ID-SIRTII	>operation unit
Japan:	NISC (National Information Security Center), METI, IPA, JPCERT/CC	>policy making unit + operation unit
Hong Kong:	Office of the Government Chief Information Officer (OGCIO) and Security Bureau	>policy making unit + operation unit
Malaysia:	MAMPU, Malaysia Cyber Security Center under Ministry of Science and Innovation, GCERT	>policy making unit + operation unit
Mongolia:	Information and Communication Technology Authority, Mongolian Cyber Incident Response Team (MONCIRT)	>policy making unit + operation unit
Philippines:	National Cyber Coordinator Office (Office of the Presidential Situation Room and Commission on Information and Communications Technology)	>policy making unit + operation unit
Sri-Lanka:	Information and Communication Technology Agency of Sri-Lanka, Sri-Lanka CERT and Tech CERT	>policy making unit + operation unit

Is it functional? Are cross governmental organizations is formed?
Is it involving private sector?

Legislation as deterrent effects in each country:

Bangladesh: computer council acts

India: information technology act 2000: amended for data security, data protection, IT offences / providing framework for recognition, issue and affixing of digital/electronic signatures and certification services / information technology act together with indian penal code

Indonesia: law on the information and electronic transactions 2008, law on telecommunications 1999, government regulation 2000: telecommunications organization, law on telecommunication 1999

Japan: act on protection of personal information 2005, act on specified commercial transactions 2002: anti spam measures, act on regulation of transmission of specified electronic mail: anti spam measures 2002, unfair competition prevention act: trade secret protection, financial instruments and exchange law: internal control on financial reporting 2007, act on electric signature and certification services / act on prohibition of unauthorized computer access, penal codes: obstruction of business by damaging a computer, computer fraud, unauthorized creation of electromagnetic records (under discussion)

Hong Kong: electronic transactions ordinance, personal data (privacy) ordinance, unsolicited electronic messages ordinance / computer crime bill incorporated in (telecommunications ordinance, crimes ordinance, theft ordinance, control of obscene and indecent articles ordinance, copy right ordinance

Malaysia: electronic government activities act 2007, communications and multimedia act 1998, communications and multimedia commission act 1998, digital signature act 1997, computer crime act 1997, telemedicine act 1997, copyright act (amendment) 1997

Mongolia: telecommunication act, state confidentiality law, privacy act are in force / criminal law is in force

Philippines: e-commerce act is in force / cybercrime prevention act, anti-telecom fraud act, data protection act are pending

Sri-Lanka: intellectual property act, electronic transaction act, computer crimes act are in force / data protection code is under way.

Can conservative legislation of the country catch up with rapidly evolved cybercrime?

(In Japan, creating and distributing a computer virus is not a crime?)

On the other hand, harsh legislation may hamper business activities?

Business had better protect by itself from cybercrime.

Promotion activities for government organizaitons/enterprises / individuals in each country:

Bangladesh: For business sector, national ICT exhibition is held annually.

India: For government, CERT-In conduct workshops and seminars. For business sector, Industry associations are creating awareness and data security council of India take care of implementation of security practices.

Indonesia: Free seminar and training are conducted by Department of CIT.

Japan: For business sector, free seminars are organized by METI, IP, JPCERT tax exemptions, financing are available.

Hong Kong: For business sector, information security showcase in August, information security summit in November, and government one-stop information security portal is available

Malaysia: MAMPU formulates standards, policy and guidelines and organizes seminar twice a year for government.

Mongolia: Security measure for IT procurement, computer incident response guideline and user recommendation/guideline are under development by ICTA.

Philippines: Formulation of National Cyber Security Plan, conduct of seminars/workshop for government, conduct of advocacy and awareness program for business sector, and organic operations among related organization

Sri-Lanka: ICTA and SLCERT jointly conduct awareness programs for government organizations and many events for cyber security week in October.

Some countries report budget constraints and shortage of human resources for promotion activities.

Introduction of ISMS (Information Security Management System) :

Bangladesh: Adopted ISO27001

India: Adopted ISO27001 40organizations ISO 27002

Indonesia: Adopted ISO27001 draft ISO27002 discussion stage

Japan: Adopted ISO27001 2500entities ISO27002

Hong Kong: Adopted ISO27001

Malaysia: Adopted ISO27001 26entities

Mongolia: Adopted MNS/ISO27001

Philippines: Incorporated in the National Cyber Security Plan for adoption and implementation

Sri-Lanka: Facilitating development of information security policies and setting up of ISMS aligned to ISO27002 in government organizations. Several Organizations are certified.

International standardization ISO/IEC27001 (ISMS requirements) and 27002 (ISMS best practice) are adopted in Asian countries.

Close-up issues for panel discussion:

How international cooperation is being built now and in future?

For challenging corporation among Asian countries to improve information security level

-Economic relationship has been deepened among Asian countries through trading, investment and business outsourcing.

-One of the business environments/infrastructures necessary for economic activities is information security in each country.

-Asia-wide tackling with information security is expected in order to raise up the bottom neck.

- -introducing requirements of Japanese enterprises
- -introducing best practices/experiences of advanced countries
- -promotion and human resource development
- -activation of information/opinion exchanges