Topic 2: Privacy Protection and Ensuring Security of Network Applications or Services

2.1 e-Commerce Security

Presented by:
Mr. Ye, Yun-Long
Director of the Department of Commerce
Ministry of Economic Affairs
August 19th, 2009

MOEA

Agenda

- Framework Summary
- Ch.1 Policy Vision
- Ch.2 Analyses of Current Situation
- Ch.3 Trends of Development
- Ch.4 **Fundamental Strategies**
- **Ch.5 Action Plans**
- **Ch.6 Issues for Discussion**

Framework Summary

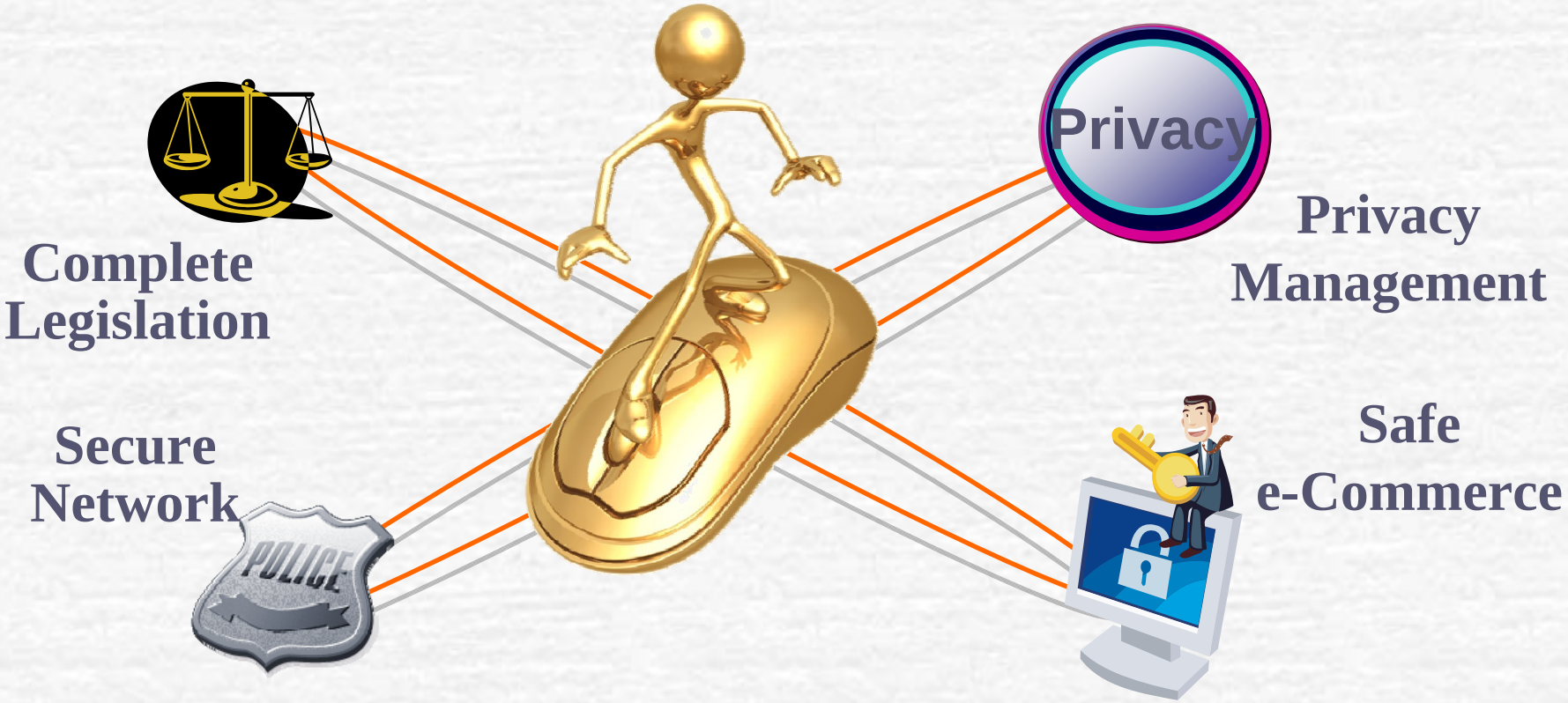
- **Strengthening Privacy Protection and Management in e-Commerce**
  1. **Aspect of Privacy Legislation:** reinforce implementation of the legal system of personal information protection.
  2. **Aspect of Privacy Management:** assist businesses to properly manage application of personal information.
- **Reinforce the Overall Transaction Security of E-commerce**
  1. **Aspect of Transaction Parties:** verify the identities of the traction parties.
  2. **Aspect of Information Transmission:** verify the authenticity and ensure the security of transaction information.
  3. **Aspect of Environment:** ensure the security of the transaction platform, payment mechanism, and goods delivery.
  4. **Aspect of Security Legislation:** reinforce e-commerce security related legal system.

MOEA

Ch.1 Policy Vision

Ch.1 Policy Vision

- Steady Confidence of Law & Reinforce Protection of Personal Information

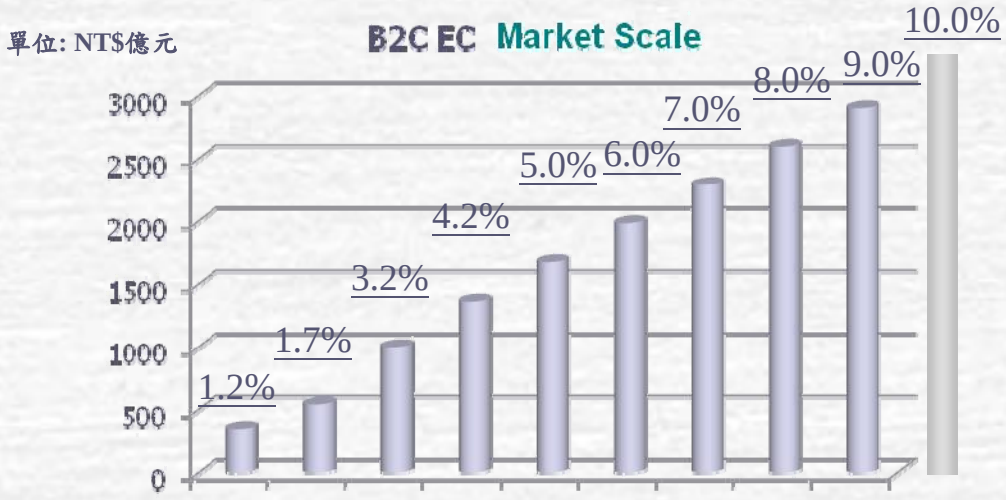


- Easy Join Secure Network & Ensure Thriving e-Commerce

MOEA

- Ch.2 Analyses of Current Situation

Ch.2 Analyses of Current Situation(1/5)



Reference:
E-commerce team, Industry For Support Division, III
2008 E-Commerce Legal System and Infrastructure Plan

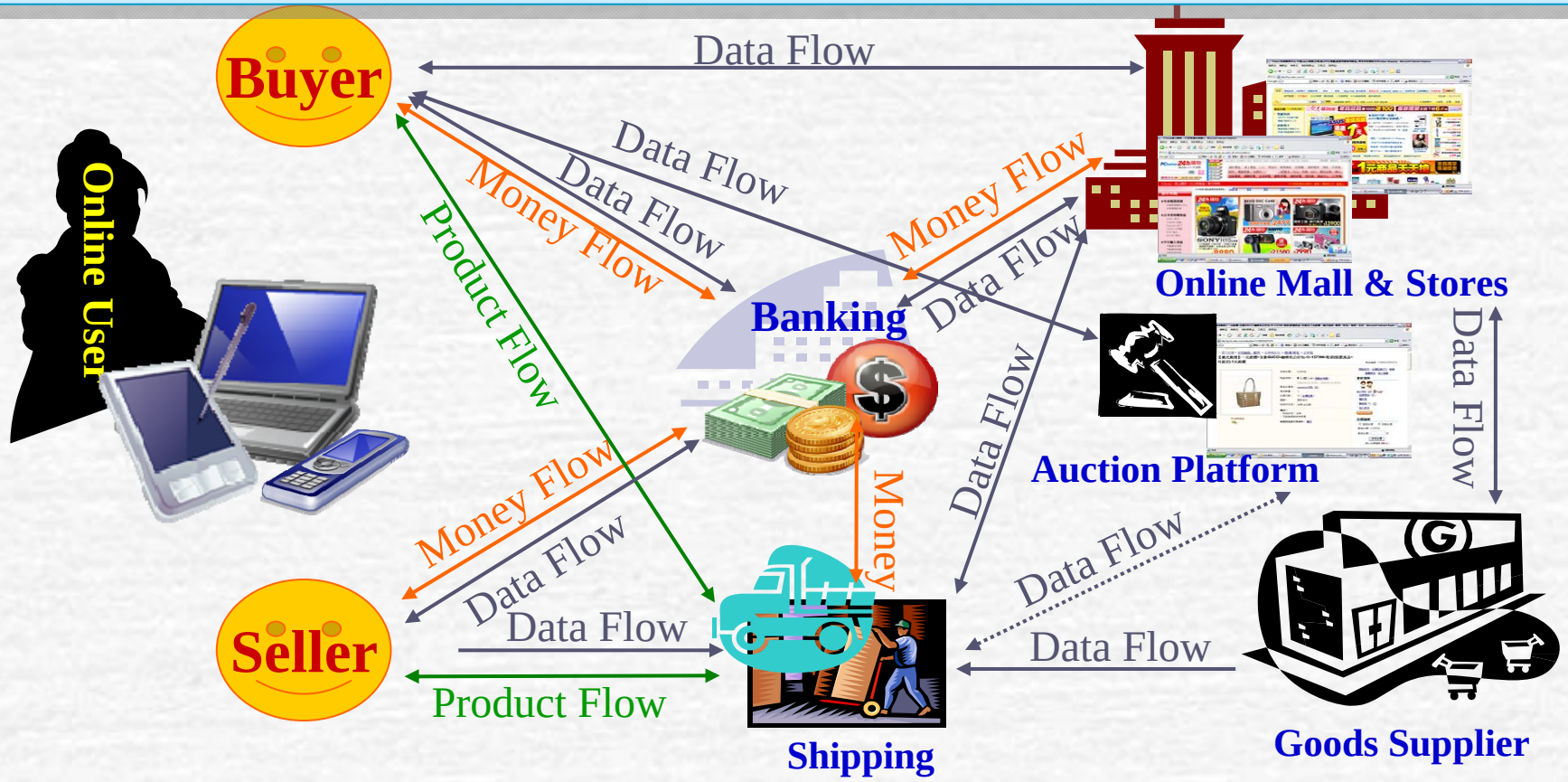
	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
B2C EC Market Scale:	347	542	1,002	1,365	1,678	1,986	2,294	2,600	2,905	3,500
Share in the Retail Market %:	1.2%	1.7%	3.2%	4.2%	5.0%	6%	7%	8%	9%	10%
C2C EC Market Scale：	--	--	--	774	1,072	1,469	2,000	2,720	3,700	4,200

- **In 2008, the B2C E-Store market scale in Taiwan amounted to NT$167.800 billion, and it is expected to reach NT$350 billion in 2013 and 14.7% of compounded annual growth rate within 4 years.**
- **In 2008, the value of the overall retail market in Taiwan was calculated at NT$3260.2 billion, and the scale of B2C E-Stores took up 5% of the overall retail market.**
- **Currently, there are estimated 19,448 online stores in Taiwan (least 16,352 and most 22,674).**
- **According to a 2008 survey, approximately 24% of the online stores have been established on independent websites, 48% affiliated to online platforms, and 28% adopted both modes. Therefore, in addition to the security of the online platforms, 52% of the websites require independent security reinforcement, and 48% to 76% require reinforcement in the security of the online platforms.**

Ch.2 Analyses of Current Situation(2/5)

The Fundamental Activities of E-Commerce (B2C and C2C)

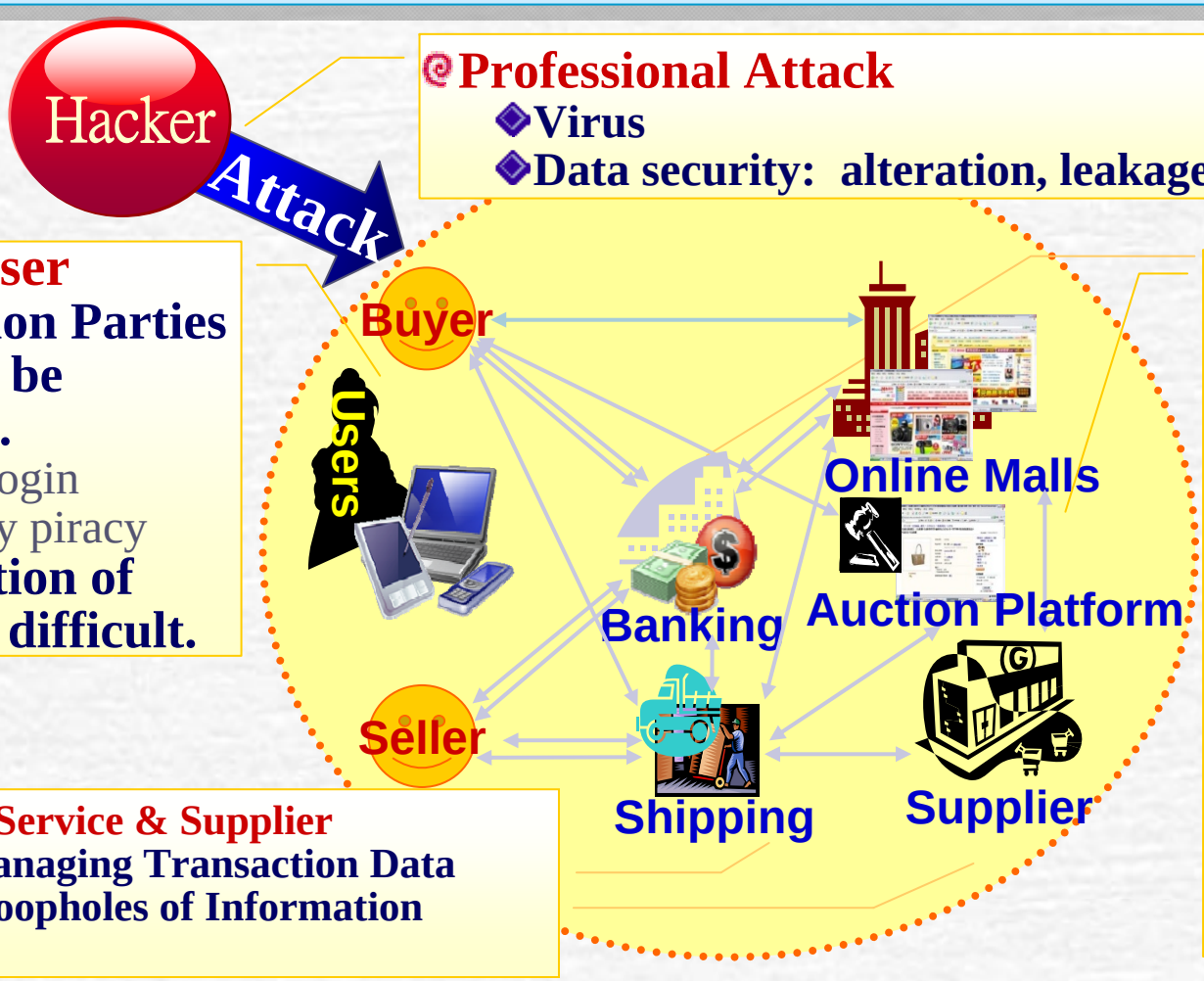
- Different from traditional transactions, the process of transaction involves multiple participants.
- E-commerce activities involve online users, online stores or auction platforms, goods suppliers, and banking/logistic services.
- During the transactions, personal information, banking information, and product information are streamed through the network and each link requires prevention and solutions to counter data leakage, info hijacking, and identity piracy.



Ch.2 Analyses of Current Situation(3/5)

Overview of e-Commerce Security

- Overall security threats appearing in the practice of e-commerce involve security loopholes in the transaction activities and professional hacker attack.
- This conference aims discuss strategies for countering security problems in the transaction activities (please see the chart below).



Professional Attack
- Virus
- Data security: alteration, leakage, and lost.

Online User
- Transaction Parties uneasy to be identified.
  - False login
  - Identity piracy
- Investigation of Frauds is difficult.

e-Store, Platform, and Money Flow
- False transaction info
  - Intercepted mail
  - Phishing website
- Transaction data intercepted for ill purposes; identity piracy causes troubles or loss.
  - False Many Transferring
  - Harassed by crime organization

Shipping Service & Supplier
- Poorly Managing Transaction Data Caused Loopholes of Information Leakage .

Ch.2 Analyses of Current Situation(4/5)

Major Incidents of E-Commerce Security

1、Aspect of Platform

- In June 2009, 8,000 entries of personal information were leaked from a TV shopping network and sold at NT$0.5 per entry online.
- In Nov. 2007, 400 entries of online member order were leaked from an online bookstore.

2、Shipping & Supplier

- Feb. 2008, online bookstore leaked out 6,000 entries of member data; the police suspected the shipping service or supplier.

3、Hacker Attack

- In Aug. 2008, a gang of hackers invaded an online bank and stole several million dollars.
- In Dec. 2007, a hacker successfully obtained 5,467 entries of member data from a shopping network through data puzzling.

4、Malware & Phishing Sites

- In Mar. 2008, a research discovered that malware was hidden in 20% of the 3,000 most frequently visited websites in Taiwan, which is often the cause of data leakage.
- In Oct. 2007, malicious links of phishing web pages appeared in an auction platform and tricked many users.

Ch.2 Analyses of Current Situation(5/5)

Outline of Urgent E-Commerce Data Security Problems

- In summary, there are in general two categories of e-commerce security problems, internal personal privacy management problem of the online stores and data security risks in each link of the transaction process, which can be further discussed through the sub-dimensions of two topics- "**Strengthening Privacy Protection and Management in e-Commerce**" and "**Reinforcing overall transaction security**".

Strengthening Privacy Protection and Management in EC

- **Privacy Legislation**
  - e-Commerce industries was not taken into consideration at the time when the current "Computer Processing Personal Information Protection Law" was drafted.
- **Practical Management**
  - Frequent occurrence of personal data leakage incidents in e-commerce related industries.
  - The industries do not know how to effectively enforce privacy protection.

Reinforcing overall transaction security

- **Transaction Parties**
  - Difficult to identify transaction parties.
- **Information Transmission**
  - False transaction information
  - High jacked transaction data
- **Environment**
  - Security loophole of platform
  - Security management issues related to Platform or Process of Money Flow
  - Uncompleted security scheme of enterprises
- **Security Legislation**
  - Uncompleted legal framework

MOEA

- Ch.3 Trends of Development

Ch.3 Tends of Development—Overview

- International organizations and many countries have begun to pay close attention to the development of personal privacy protection and management, and legislations, as well as establishment of personal privacy management systems have also taken place.
- Many countries are very serious about the security of e-transactions and have begun legislation to regulate or encourage corporations to establish or initiate relevant mechanisms or self regulations to uplift the security of e-transactions.

e-Commerce Privacy Protection/ Management

Privacy Legislation

International:
- ✓ Legislation/amendment of personal information laws (i.e. chart page 14)
- ✓ International Organizations (APEC, OECD, EU)

Domestic:
- ✓ Relevant regulations are under legislation/amendment (Personal Information Law, Enforcement Rules for Key Industries Computer Processing Personal Information)

Privacy Management

International:
- ✓ Establishment of personal information management system (i.e.: Japan, Korea, Germany)

Domestic:
- ✓ Personal Info. Management System is not yet established.
- ✓ Necessity to establish the management system for adaptation to the changes of law.

E-Commerce Overall Transaction Security

Transaction Parties

- Some countries legislate to enforce certification on all e-commerce transactions (i.e. South Korea's E-commerce Basic Law)
- Businesses voluntarily adapt identity confirmation mechanisms (i.e. security seal, digital certificate, mobile phone ID verification)
- 20.8% of online stores think transaction security and certification mechanisms in Taiwan are worrisome.

Environment

- Website security reinforcement mechanism are taken seriously (i.e. weak spot detection, hacker blocking mechanism)
- Enterprises' internal security scheme not yet complete (i.e. establishment of Chief Information Security Officer "CISO").
- Initiation of online banking security mechanism (i.e. dynamic password and banking certifications)

Data Transmission

- Businesses voluntarily established false transaction prevention mechanisms (SSL encryption, encrypted email, encrypted hard-disk data)
- 36.1% domestic online stores think fraud lowered the confidence of the consumers.

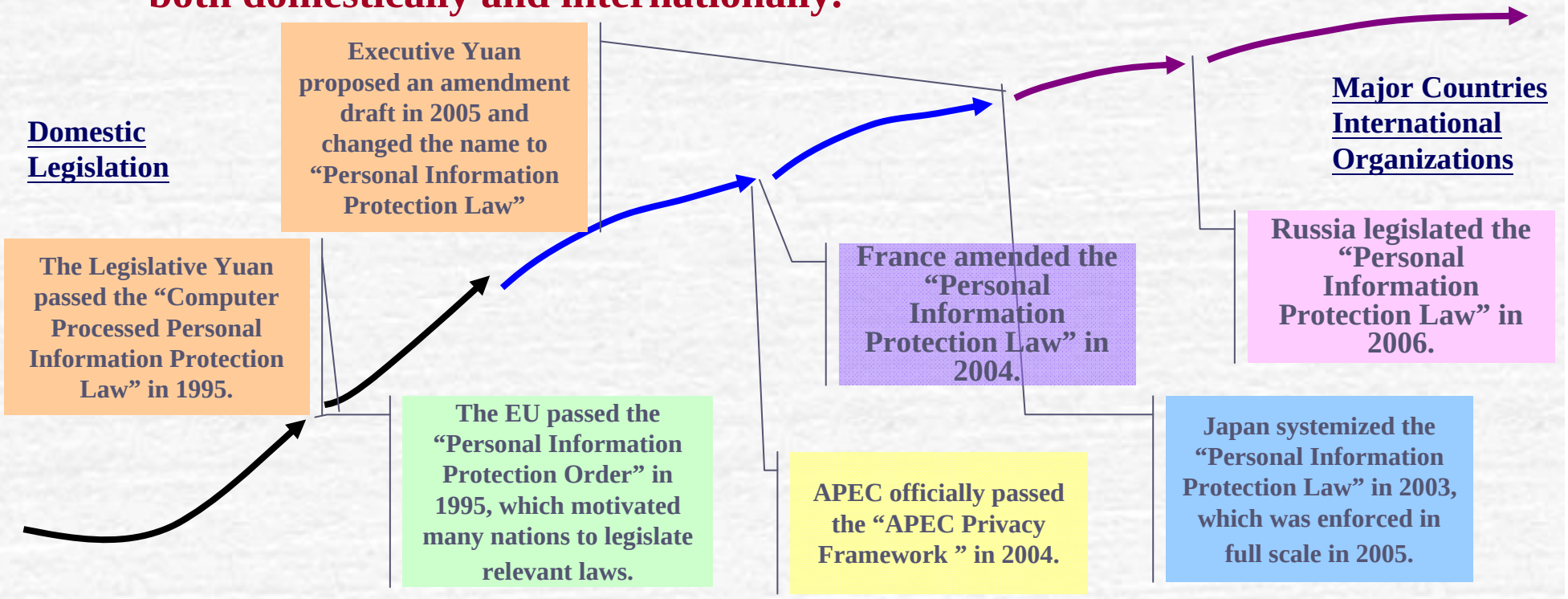
Security Legislation

- Many countries began to establish legal systems for information security control (i.e. the US, Japan, and China)
- Information security reporting system has emerged. (i.e. USA)

Ch.3 Tends of Development－Individual Discussion(1)

■ Strengthening Privacy Protection and Management in e-Commerce: Privacy Legislation

- **Legal system for protection of personal information has been taken seriously both domestically and internationally.**



- Nations continue to reinforce legislation of personal information protection. In recent years, several nations, including France, Japan, Russia, and Canada, have devoted substantial resources to draft or amend relevant regulations. A draft for amendment of the personal information Law has also been proposed in Taiwan.
- International organizations have also been emphasizing privacy protection. APEC passed APEC Privacy Framework in 2004 and began to enforce the "Pathfinder Program", requesting its members, including Taiwan, to initiate and follow the relevant stipulations.

Ch.3 Tends of Development—Individual Discussion(2)

■ Strengthening Privacy Protection and Management in e-Commerce: Privacy Management

Personal Information Protection Management System-Japan

- Japan highly values the protection of personal information. In addition to law making, Japan has also enforced the "Personal Information Management System" in conformity with the law (JIS Q 15001:2006)
- The Japanese Ministry of Economy, Trade, and Industry (METI) assisted the Japan Information Processing Development Corporation (JIPDEC) to promote the P-Mark System, which was established based on its own personal information management system; up to date, over 10 thousand companies have been certified.

Personal Information Protection Law (passed in 2003 and enforced in 2005)

↓

The Basic Principles of the Personal Information Protection Law (2005)

↓

Personal Information Management System JIS Q 15001: 2006

↓

Japan Information Processing Development Corporation (JIPDEC)

- ✓ Establishment and amendment of the management system
- ✓ Maintenance of system operation
- ✓ Identity verification by the certification organization
- ✓ P-Mark Issuing

- ✓ The system was established under government project consultation at the initial stage and is now under self operation status.

Certification Organization (Industry Organizations/ Associations)

Certification Organization (Regional Organizations/ Groups)

Consultation Organization

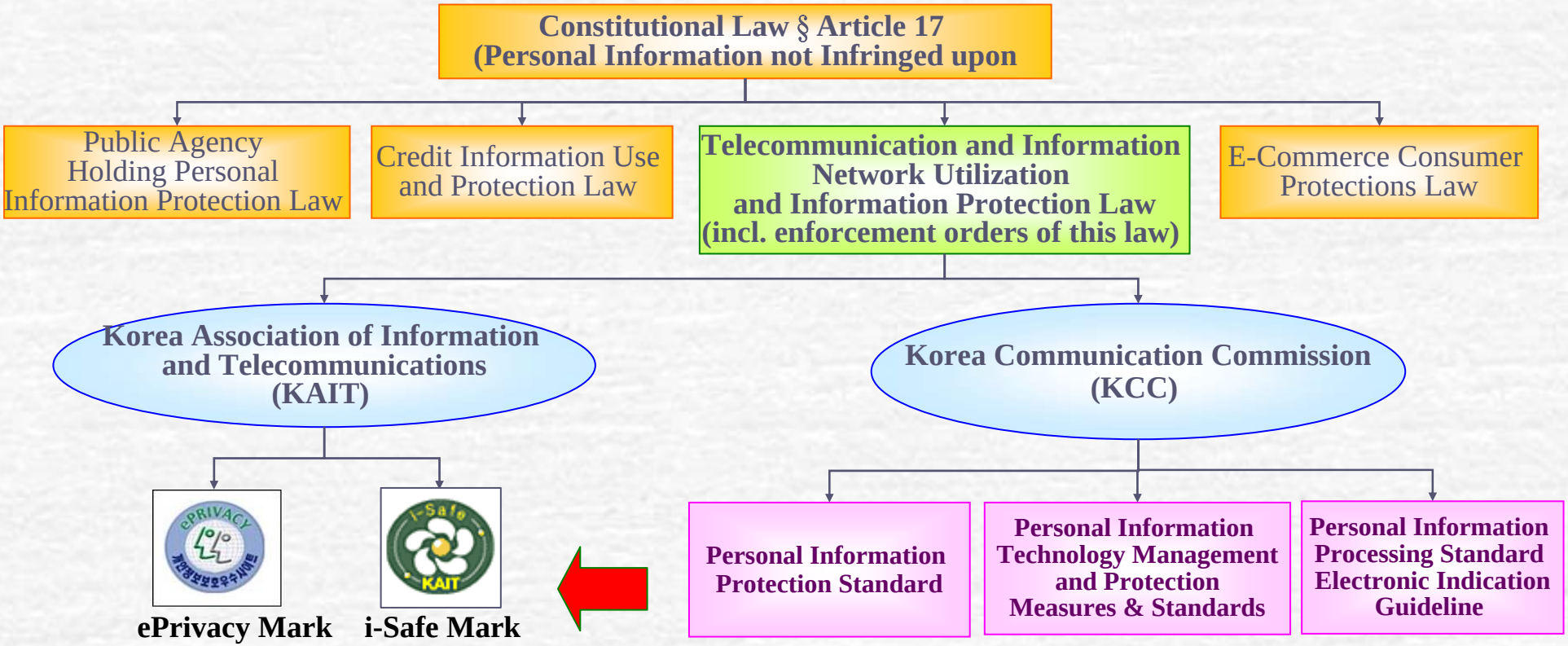
International Recognition

Ch.3 Tends of Development—Individual Discussion(3)

■ Strengthening Privacy Protection and Management in e-Commerce: Privacy Management

Personal Information Protection Management System-Korea

- South Korea regulates its internet personal information protection issues and promotes privacy management system through the "Telecommunication and Information Network Utilization and Information Protection Law" and issues the ePrivacy Mark.
- Currently, the most trusted privacy management system was established by the Korea Association of Information and Telecommunications (KAIT), which is directly supervised under the President by the Korea Communication Commission (KCC).

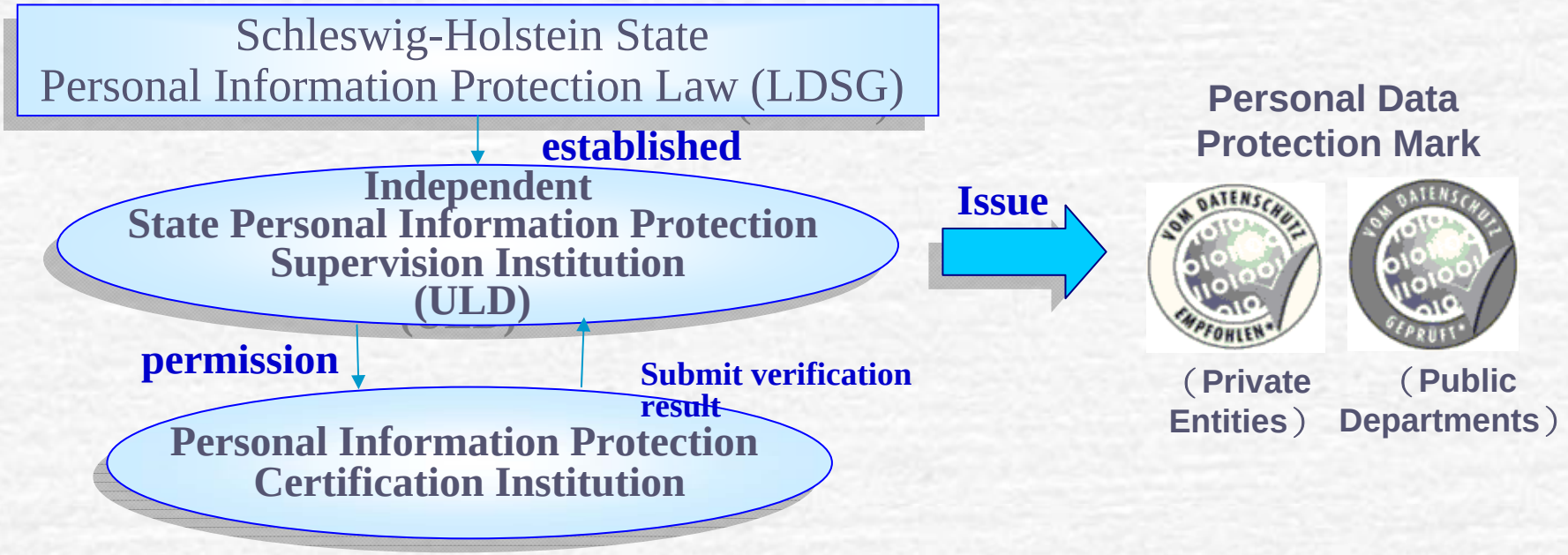


Ch.3 Tends of Development－Individual Discussion(4)

■ Strengthening Privacy Protection and Management in e-Commerce: Privacy Management

Personal Information Protection Management System-Germany

- To consolidate personal information protection regulations of the member nations, the EU passed the Directive on Data Protection and the Electronic Telecommunication Privacy Directive, which served as frameworks for the member nations.
- Germany has also legislated at the federal level Personal Information Protection Certification Law and is expected to begin nationwide enforcement of the personal information management system from 2010. It is the pioneer of personal information system management system of the world.
- At the current stage, several states in Germany have voluntarily launched Personal Information Protection Certification Systems; all those that pass the certification process are given a personal information protection mark.



■ Comparison of Personal Information Management System in Japan, Germany, and South Korea

Item	Japan	Korea	Germany
Major Legislations	Personal Information Protection Law	Telecommunication & Information Network Utilization and Information Protection Law and relevant regulations	Federal Personal Information Protection Law; Federal Personal Information Protection Certification Law
Contents of Laws	Corporations' responsibilities for Personal Information Protection.	Website operators and online businesses are responsible for Personal Information Protection	Regulate the authority, the certification agency, and the process.
Mark Issuing	P-Mark	ePrivacy-Mark	Personal Information Protection Mark
Scope of Application	Corporate management of personal information	Management of Personal Information collected from the internet and held by corporations.	Protection plan put forward by corporations and the telecommunication/ communication products and services offered.
Management System/Certification Organization	Japan Information Processing Development Corporation (JIPDEC)	Korea Association of Information & Technology (KAIT)	Personal Information Protection Certification Institutions
Maintenance of Operations	Initial Stage: Government funding Stable Stages: Self Operation	Established based on relevant laws and funded by government budget.	Self Operation

- Although Enterprises adopting information management system is not mandatory by law, the system could serves as a standard, which helps the corporations to set up their own systems and build customer trust, and an indicator by which the judicial system makes judgments in personal information security related disputes.
- Even though setting up personal information system is not always required by law around the world, it is still should be considered the necessity to regulate it as a mandatory requirement for the purpose to fit our national condition to enhance the efficiency of the system.
- Management and certification systems of these three nations are implemented by private organizations. The Japanese system (at the initial stage) and Korean systems are funded by government budgets; this shows that the government plays an important role in effective implementation of personal information protection.

■ Reinforcing Overall E-Commerce Transaction Security : Transaction Parties

- South Korea passed the “E-Commerce Fundamental Law” and stipulated mandatory use of digital certificate by the transaction parties to ensure the authenticity of the identities and transaction information at the two-sides of transactions.
- To reinforce the security of certification and build public trust, certification mark systems are implemented for easy identification in South Korea.

E-Commerce Basic Law

Online Banking
- ✓ Used by online bank account holders of 19 South Korean banks and post office.

Online Shopping
- ✓ Pay by credit card
- ✓ Over 300,000 Won

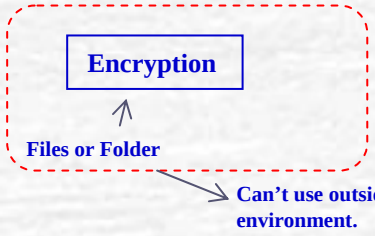
Online Order
- ✓ Online Securities Subscription

South Korea’s CA Trust Mark

Reference: Korea Information Safety Association (KISA)

■ Reinforcing Overall E-Commerce Transaction Security : Data Transmission

- Major countries and international organizations emphasize the transition of information security.
  - In 2008, election of committee Davidson county Tennessee State U.S lost two Notebook, which 337 thousand voter's social security number loss. In March 2009, another 22 thousand credit card number stolen from Google searching engine. That's reason the nations are looking for the well protected data encryption, make data useless in non-authority environment. Recently, many data security supplier in States are developing files and file folder encryption, as well as Database encryption. In order to prevent this crisis.
  - The worlds are threatened by tons of spam, phishing and pornography e-mails. According to white paper of internet security, published by Message Labs of Symantec in June. The spam emails increase 8.6% in June, France. Which become the most spam email countries in the world. In US, decrease 23.6%, In Canada, decrease 27.8%. In UK, increased 10.3%. In German, increase 4%, In Holland, decreased 6.1%. In Australia, decreased 11.2%. In Japan, decreased 23.9%. That's why US are developing ID verification system of registered email.



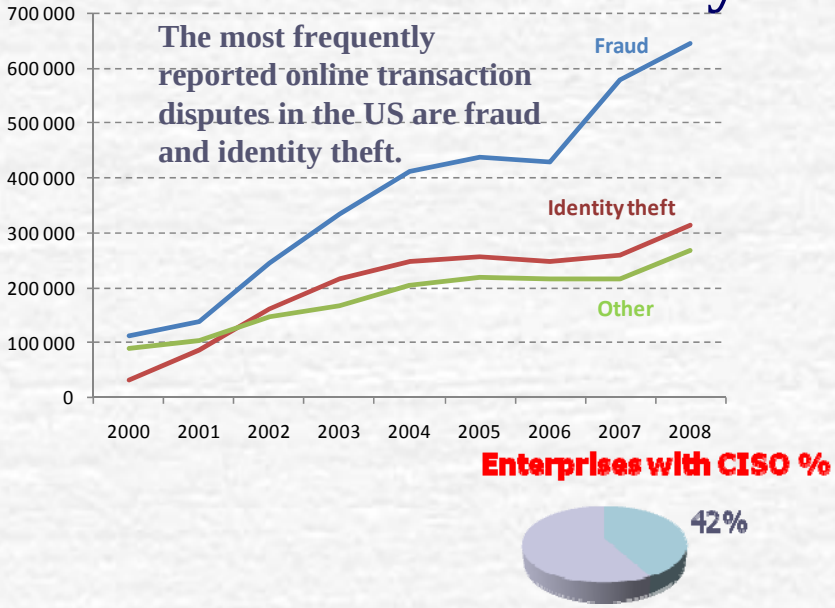
The trend for the information transmission should focus on data encryption and protected while transited.

- Beside information security system, business also pays much attention on data encryption. Especially to ensure the security when date transmission externally. Decrease the possible damage comes from the data loss.
- The whole world are looking for anti-spam email, anti-phishing, anti-virus and spam against email system, which hope to establish a trustable and safe email system such as registered email system.

Ch.3 Tends of Development－ Individual Discussion(8)

■ Reinforcing Overall E-Commerce Transaction Security : Environment

- **Major countries and international organizations emphasize building public trust in ICT.**
  - EU i-2010 Program
  - Japan u-Japan Program
  - The US Government has considered using preferred tax terms to drive forward the development of information security software
  - APEC actively initiated cross-border privacy protection work team conferences (Taiwan also participated).



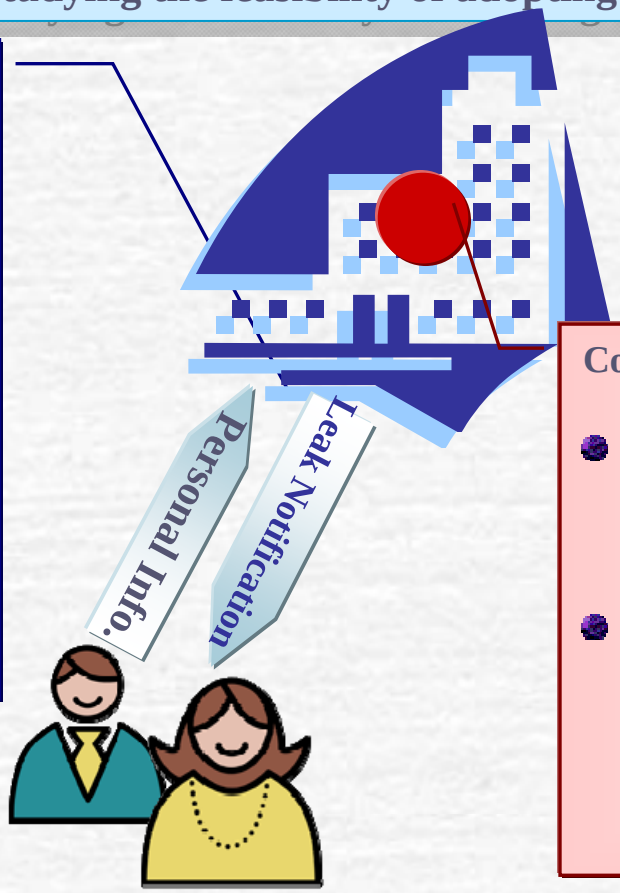
- **EU (i-2010 Program) mentioned "Trust and Reliance": "Wide-spread internet application should be established on top of a network trusted by people."**
- **The U-Japan Program also has concerns of how to build public trust in ICT when the internet environment becomes inextricably linked into people's lives.**
- **Since 2001,US Government has encouraged enterprises to implement the position of Chief information security Officer. After the 9/11 attacks, US Government started to encourage enterprise to implement the position of Chief Security Officer. According to the survey of CSO magazine on March 2005, Almost 42% of enterprises had implemented CSO position .**
- **When the US attempted to propose stimulation plans to the software companies in order to upgrade the level of information security, members of the Senate proposed preferred tax terms to encourage the development of information security standard compliant software.**
- **President Obama stressed that the government should work more closely with private organizations. He pointed out that a large portion of the nation's digital infrastructure is privately owned, so the policy makers should work effectively with industrial leaders to build a coordinated security guarding mechanism.**

■ Reinforcing Overall E-Commerce Transaction Security : Security Legislation

- Internationally, legal systems regulating corporations include information security control systems that regulate the corporations internally, as well as reporting systems for information security incidents that have already taken place.
- Information leak reporting system has been passed in California, USA in 2002, which mandates corporations to inform the involved parties during an information leak incident. EU, Australia, and New Zealand are also studying the feasibility of adopting this system.

USA Legislation: California for Example

- Organization where information leak occurred must inform the parties involved in writing or through email.
- In the case when over 500,000 persons are affected or the cost for notification exceeds US$250,000, notifications can be made through email in conjunction with website and media release to replace written notification.



Corporate Internal Information Security Control System

- After the Enron case, information security control issues emerged from false financial reports began to gain wide attention.
- Many countries began to legislate relevant regulations, i.e. the Sarbanes-Oxley Act of the US, the Financial Instruments and Exchange Act of Japan, and Corporate Internal Control Basic Standard of China.

MOEA

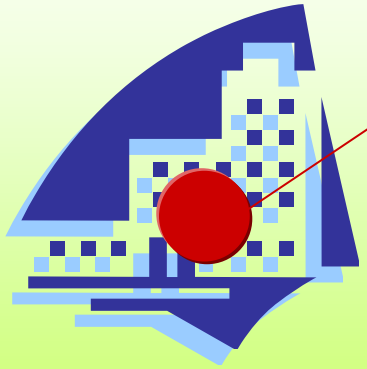
- Ch.4 **Fundamental Strategies**

CH.4 Fundamental Strategies (1)

■ Strengthening Privacy Protection and Management in e-Commerce

- In respect of legal system & policies, Personal Data Protection Law must be passed as soon as possible, and relevant key industries which have necessity to enhance protection policy of personal data should be appointed to follow current law during this transitional period to provide the public with sufficient legal protection.
- In addition to build a comprehensive legal system, to corporations strengthen their internal personal information management system to meet the legal requirements is also deemed important. To achieve these goals, the government should construct a personal information management system and coordinates the system with privacy marks for maximum effectiveness.

Personal Information protection Structure



External

Privacy Legislation

Comprehensive personal information protection legal system to ensure effective enforcement of privacy protection programs

Internal

Privacy Management

Establish a personal information protection and management system with coordinated privacy marks mechanism.

✓**Expected effects:** Minimize the frequency of personal information leakage
Urge the industry to pay maximum attention to personal information protection
Promote development of personal information management related industries

CH.4 Fundamental Strategies (2)

■ Reinforcing Overall E-Commerce Transaction Security

- Overall e-transaction security: information security through the whole process of a transaction, from the initial identity confirmation at both sides to order, payment, and delivery, must be assured and maintained at all times.
- Reinforce transaction security: in addition to protecting the rights of the two sides in a transaction and securing the reputation of the business, reinforced security will build public trust to e-commerce and in turn stimulate business growth through e-transactions.

Preparation	E-Commerce Activities	
	Transactions	Data Transmission, Environment, Legislation
• Reinforce consumer recognition of trust and security. • Promote fraud prevention and online transaction security to the consumers and stores.	• Push forward application of online transaction electronic certification. • Establish e-commerce website authenticity confirmation mechanism.	• Promote trust and security mechanisms through policy tools. • Promote online transaction platform security mechanism.	• Establish online banking security reinforcement mechanism. • Promote establishment of e-commerce trust and security backup center. • Coordinate legal systems.

Online Mall

Auction Platform

Banking Services

Suppliers

Shipping Service

Reinforce cognition of the users

Build a secured transaction mechanism to upgrade the trust and security of the transaction environment. Coordinate with government policy tools and mechanisms to ensure wide application of e-commerce security mechanism.

MOEA

Ch.5 Action Plans

Ch.5 Action Plans – STRUCTURE

■ Strengthening Privacy Protection and Management in e-Commerce

Privacy Legislation

- **Implement Personal Privacy Protection Programs**
  - **(1)** Legislate personal information laws and coordinated standards.
  - **(2)** Study and plan a personal information protection system
  - **(3)** Personal information promotion and education

Privacy Management

- **Establish Personal Information Management System**
  - **(1)** Set up personal information management system in accordance to the legal regulations.
  - **(2)** Establish coordinated privacy mark system.
  - **(3)** Promote cross-national or mutual-recognition certification model.

■ Reinforcing Overall E-Commerce Transaction Security

Transaction Parties

- **Promote transaction party confirmation mechanism**
  - **(1)** Reinforce application of online transaction certification.
  - **(2)** Promote e-commerce website confirmation mechanism
- **Promote Transaction Security Knowledge and Reinforce Cognition**
  - **(1)**Reinforce and promote consumer transaction security knowledge.
  - **(2)**Reinforce education on fraud and online transaction crime prevention.

Data Transmission

- **Ensure Wide Application of E-Commerce Trust Security Mechanism**
  - **(1)** Plan for R&D of security mechanism and professional training programs.
  - **(2)** Promote e-commerce trust security mechanism.
  - **(3)** Continuously upgrade the retailers' information security quality.

Environment

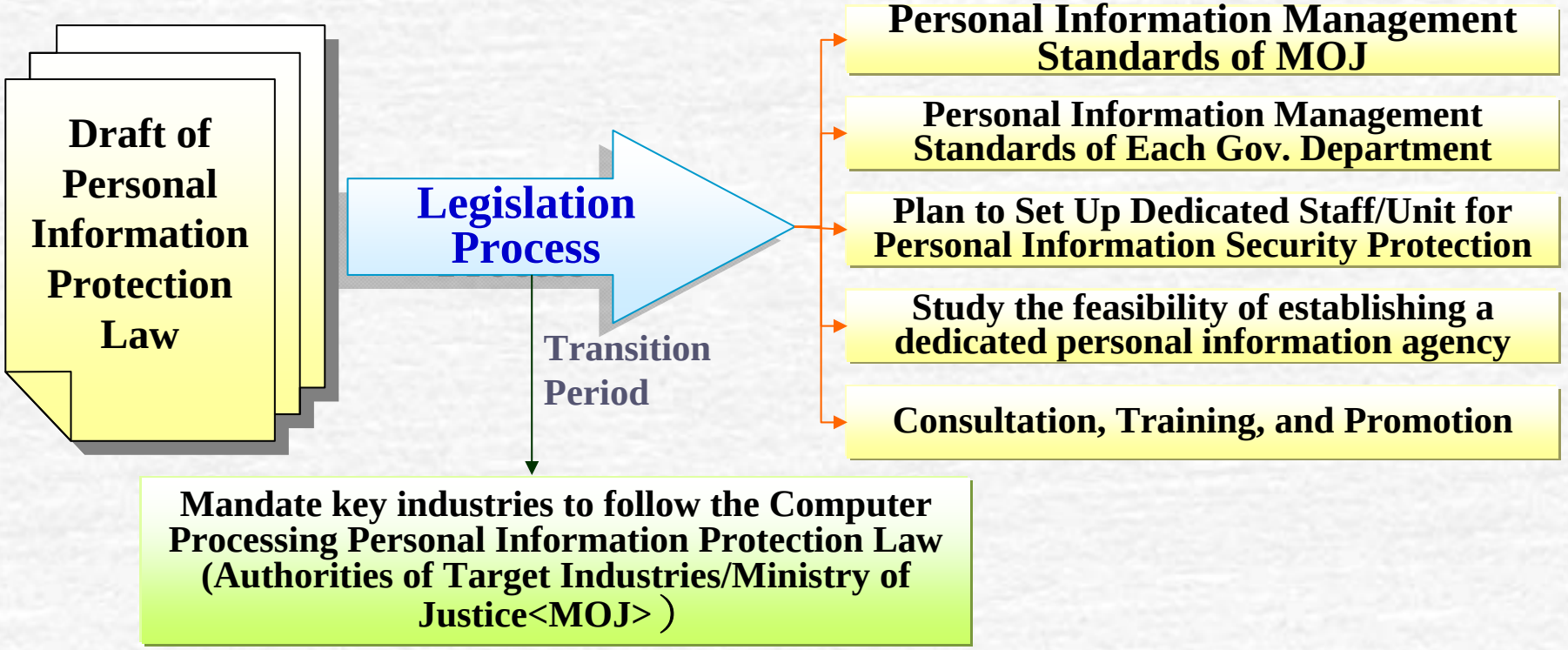
- **Promote Online Transaction Platform Security Mechanism**
  - **(1)** Assist businesses to establish anti-hacker personal information interception mechanism.
  - **(2)** Establish an e-commerce supplier trust security standard.
  - **(3)** Establish e-commerce logistic service provider trust security standard.
- **Promote E-Commerce Trust Security Backup Mechanism**
  - **(1)** Establish e-commerce trust security detection and diagnostic mechanism
  - **(2)** Establish e-commerce information security reporting platform.
  - **(3)** Provide e-commerce trust security consultation service.
  - **(4)** Organize e-commerce trust security service alliance.
  - **(5)** Promote international cooperation in e-commerce trust security.
  - **(6)** Train the seed of Information security employees & CISOs

Security Legislation

- **Draft/Amend Electronic Certification related Transaction Security Standards**
- **Promote Corporate Information Security Control Standards.**

Ch.5 Action Plans－Sub-plan (1)

- **Strengthening Privacy Protection and Management in e-Commerce －Privacy Legislation**
  - **Implement Personal Privacy Protection Programs (MOJ)**

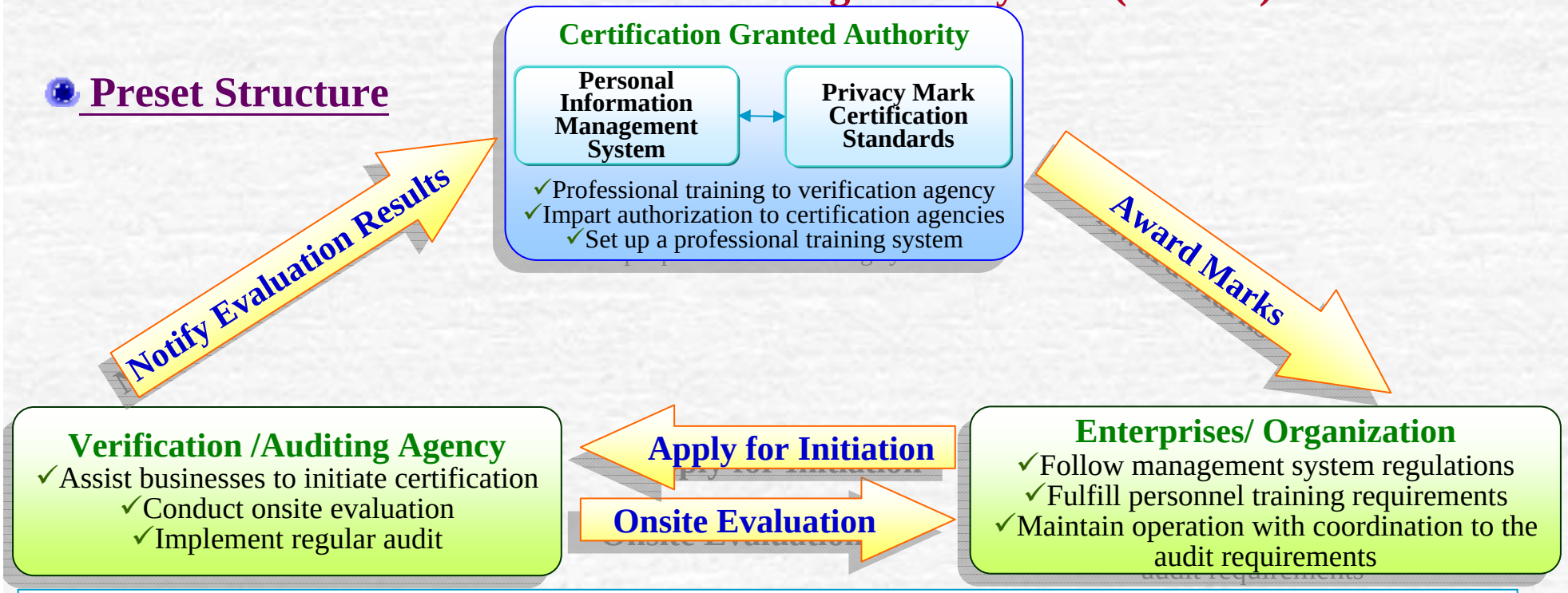


- Establish a comprehensive personal information protection legal system to assist public and non-public organizations in setting up proper protection measures, and at the same time help the public offices to lay out relevant regulations and systems in respond to the changes in the personal information protection law system
- A comprehensive system needs coordinated education and promotion in order to ensure a wide application. Therefore, training and education will be launched in this program to maximize the effectiveness of legal system implementation.

Ch.5 Action Plans－Sub-plan (2)

- **Strengthening Privacy Protection and Management in e-Commerce －Privacy Management**
  - **Establish Personal Information Management System (MOEA)**

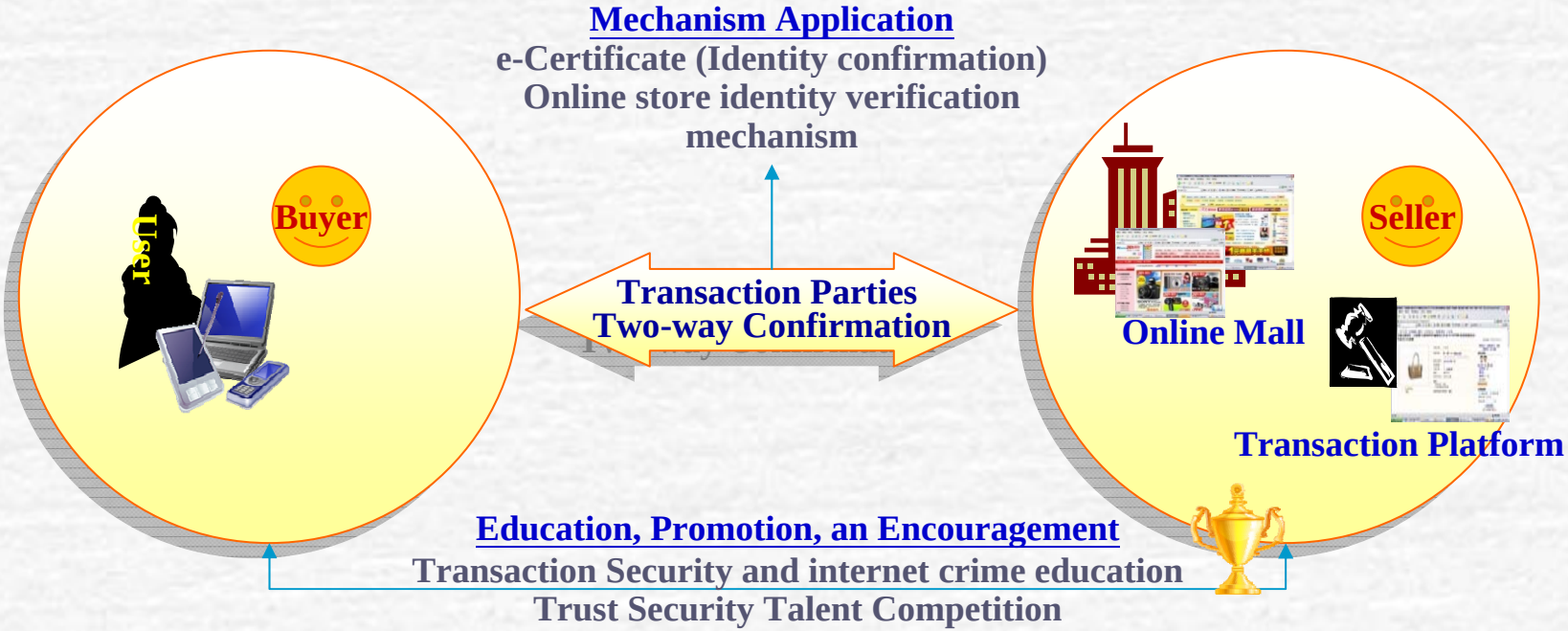
Preset Structure



- Establish the Nation's personal information management system and coordinated privacy marks system with reference to international privacy protection systems and international requirements (i.e. APEC, OECD).
- A neutral third party assumes the duty as "Certification Granted Authority", which studies and maintains the management system. Qualified information service entities or industry associations serve as the verification agency to help the businesses to set up management systems and conduct regular audit.
- Establish a professional training system, plan and develop agency audit personnel and internal system set up personnel.

Ch.5 Action Plans－Sub-plan (3)

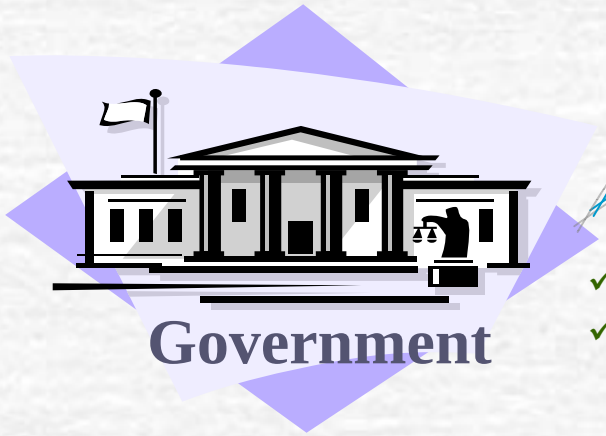
- **Reinforcing Overall E-Commerce Transaction Security－Transaction Parties**
  - **Promote transaction party verification mechanism (MOEA)**
  - **Reinforce transaction knowledge promotion and cognition (MOEA and MOI)**



- Use e-certificate and website verification mechanism to help both sides of a transaction to confirm the identities, which effectively reduces internet fraud such as false identity trading and internet phishing.
- Consider whether to assure wide application of certificate through legally mandatory requirements. (i.e. Korea)
- Reinforce instilling of online store transaction security and the basic crime prevention concepts through education, promotion, and encourage- secure the information security protection system from the root.

Ch.5 Action Plans－Sub-plan (4)

- **Reinforcing Overall E-Commerce Transaction Security－Data Transmission**
  - **Ensure Wide Application of E-Commerce Trust Security Mechanism (MOEA)**



✓ Incentive Programs
✓ Consultation & Promotion

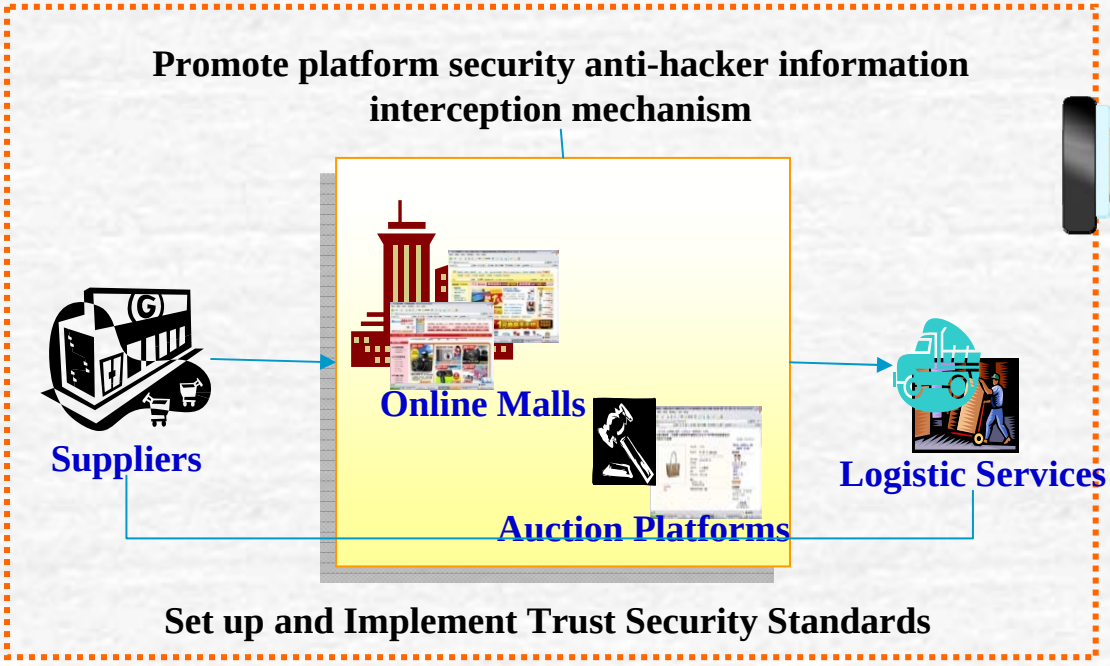
- **Mechanisms in Promotion**

Data encryption, Mail Security Mechanism, Safety Detection Mechanism, Trust Payment Mechanism

- **Use policy tools to encourage investment in e-commerce trust security mechanism & professionals development**
- **Promote the various trust security mechanisms to help the industries to set up proper e-commerce trust security mechanism。**

Ch.5 Action Plans－Sub-plan (5)

- **Reinforcing Overall E-Commerce Transaction Security－Environment**
  - **Promote online transaction platform security mechanism (MOEA)**
  - **Promote e-commerce trust security support mechanism (MOEA)**



- ✓ E-Commerce Trust Detection and Hacker Attack Reporting System.
- ✓ E-commerce Information Security Reporting Platform
- ✓ Information Security Consultation and Diagnostic Services & Participation in International Conferences
- ✓ Organize E-Commerce Trust Security Alliance
- ✓ Promote International Trust Security Cooperation
- ✓ Train the seed of Information security employees & CISOs

- **Assist e-commerce platform businesses to set up an online transaction platform security mechanism and establish trust security standards targeting suppliers and logistic service suppliers to reinforce and establish a secured trading environment.**
- **Play the role as consultant to establish e-commerce trust security support mechanism and provide the e-commerce industry various services to maintain operation of trust security; i.e. security detection and hacker reporting mechanism, consultation and diagnostic services, reporting platform, survey and statistical analysis, trust security research indicator, and international cooperation.**

◎The trust security standards of suppliers & logistics service providers are about the security criteria, internal control, system security level, access authority rule , etc.

Ch.5 Action Plans－Task Division

Plans	Main Organizers	Co-organizers
Implement Personal Privacy Protection Programs	Ministry of Justice (MOJ)	All other gov. department
Establish Personal Information Management System and coordinated privacy mark	Ministry of Economic Affairs (MOEA)	MOJ/ All other gov. departments
Promote transaction party verification mechanism	Ministry of Economic Affairs (MOEA)	All public offices
Reinforce and Promote Consumer Transaction Security Knowledge	Ministry of Economic Affairs (MOEA)	Consumer Protection Commission (CPC)/ MOI
Ensure Wide Application of E-Commerce Trust Security Mechanism	Ministry of Economic Affairs (MOEA)	
Promote online transaction platform security mechanism	Ministry of Economic Affairs (MOEA)	
Promote e-commerce trust security support mechanism	Ministry of Economic Affairs (MOEA)	All other gov. departments
Promote knowledge related to fraud prevention and internet transaction crime	Ministry of the Interior (MOI)	All other gov. departments

Ch.5 Action Plans – Full Budget Projection (Total)

Unit: Thousand NT$

Units	2010 Budget	Full Budget
Ministry of Justice	900	5,000
Ministry of Economic Affairs (Dept. Commerce)	149,550	712,000
Ministry of the Interior (National Police Agency)	56,000	206,000
Total	206,450	923,000

Ch.5 Action Plans – Full Budget Projection (by Plan)

Unit: Thousand NT$

Units	Action Plans	2010 Budget	Full Budget
Ministry of Justice	Implement Personal Privacy Protection Programs	900	5,000
Ministry of Economic Affairs (Dept. Commerce)	Establish the Nation's Personal Information Management System	31,950	215,800
	Promote transaction party verification mechanism and E-commerce Security Regulations Adaptation	17,600	96,200
	Reinforce and Promote Consumer Transaction Security Knowledge	10,880	43,520
	Ensure Wide Application of E-Commerce Trust Security Mechanism	25,080	108,080
	Promote online transaction platform security mechanism	34,900	138,900
	Promote e-commerce trust security support mechanism	29,140	109,500
Ministry of the Interior (National Police Agency)	Promote fraud and internet transaction crime knowledge	56,000	206,000

Ch.5 Action Plans – KPI and Industrial Effects

Plans	Projected Goals (KPI)	Industrial Effects
Implement Personal Privacy Protection Programs	• Complete legislation of personal information protection law • Complete Ministry of Justice personal information protection & management related standards and assist all offices to set up guidelines.	• Comprehensive legal system ascertains the standards for personal information protection and provide clear standards for easy implementation.
Establish Personal Information Management System and Coordinated Privacy Marks	• Complete the Nation's personal information management system, coordinated privacy mark system, and implementation works • Assist at least 6 evaluation agencies to obtain qualification within four years and help 100 companies to initiate the system. • Negotiate with at least one country for mutual certification recognition.	• Assist the industry to construct a management system that is compliant to the Personal Information Protection Law. • Drive forward the development of personal information management certification services and create at least NT$10 million business opportunities.
Promote transaction party verification mechanism	• Assist at least 50 online stores each year to set up the verification mechanism. • Complete the structure of the online transaction certification legal system.	• Help to expand the domestic certification application market and profit base for the certification industry.
Reinforce and Promote Consumer Transaction Security Knowledge	• Decrease internet transaction fraud rate by 2% • Organize knowledge training for minimum 1,600 persons • Select at least 20 e-commerce trust security talents from the competition.	• Provide the consumers with e-commerce trust security knowledge to effectively minimize disputes and customer complaints.
Ensure Wide Application of E-Commerce Trust Security Mechanism	• Promote E-Commerce Trust Security Mechanism, set up at 400 businesses. • Counsel at least 2000 trust e-stores. • Promote upgrade of retailer information security quality for minimum 4000 businesses. • Select minimum of 20 quality e-commerce trust security stores each year.	• Upgrade the information security quality for online stores and retail services. • Promote development of e-commerce trust security related industries. • Create at least 400 job opportunities.
Promote online transaction platform security mechanism	• Assist at least two medium to large businesses to set up anti-hacker personal information interception mechanism each year. • Assist at least 20 suppliers and 3 logistic service providers to initiate e-commerce information security standards.	• Lower the hacking rate in the online transaction platform. • Upgrade the information security quality in the key links of E-commerce to lower the risk of information leak. • Promote development of information security standard related industries.
Promote e-commerce trust security support mechanism	• Complete e-commerce trust security indicators and set up support center trust security detection system. • Complete set up of e-commerce trust security reporting mechanism • Organize e-Commerce trust security alliance. • Achieve at least one successful international e-commerce trust security cooperative venture each year.	• Maximize the effect of information security in each link of e-commerce though cooperative alliance. • Achieve NT$370 billion B2C e-commerce market scale within 4 years.

MOEA

- **Ch.6 Issues for Discussion**

MOEA

Issues for Discussion

- **The complication of overall strategies for enhancing e-Commerce security.**
- **Strengthening Privacy Protection and Management in e-Commerce**
  - Internationally, some nations legislate to mandate establishment of personal information management system, and some only require reinforcement in the responsibilities of ensuring the security of personal information. Are legal regulations necessary? Which is the better option?
  - In order to enhance the efficiency of promotion result, who should play the major role to establish and promote the personal management system under social condition in Taiwan? Government or Private Sectors?
- **Reinforcing Overall E-Commerce Transaction Security**
  - For verification of transaction parties, is it necessary to legislate mandates for use of certification in certain electronic transactions?
  - Is the planning and implementation of the e-commerce trust security support center comprehensive and does it meet the needs of the industry?

Thank you for your Attention !

MOEA

Appendixes

Comparison of the Personal Information Management System and ISO27001 Information Security Standards

Comparison	ISO 27001	Personal Information Management System
Scope of Application	Manage all “Information Assets”	Specially emphasize the specific area of “personal information” in the category of “information asset”
Standards	Based on international standards	In addition to international standard compliance, it meets the requirement of the Personal Information Protection Law system
Goals	Aims to meet international standards	Aims to fulfill the mission imparted by the Personal Information Protection Law

- **The ISO 27001 system manages “information assets” in an all-encompassing sense, but the personal information management system emphasizes protection of “personal information” and compliance to legal regulations.**
- **The personal information protection management system adopts the domestic information protection legal system; therefore, once a company is successfully initiated and certified, the company is deemed to have fulfilled the requirements of the personal information laws.**

Supplement: Response to the seminar held by the Technology Consultant Team on June 26th

Issues	Unit	Response
Enforcement of information security related regulations should be well coordinated and the difficulties in actual practice of personal information management reinforcement faced by small and medium enterprises should also be addressed.	Ministry of Economic Affairs/ Ministry of Justice	Ministry of Economic Affairs: plan grants to helps small and medium enterprises in initiation of information security and personal information management reinforcement system.
Organizations holding massive amount of personal information should be monitored by the authority in order to substantiate information protections and internet security protection.	All public offices	The draft of Personal Information Law (§22、§25) has made definition to the obligations of the target industry authorities.
In the case of information leak, the legal system should reduce the liability of organizations certified by the trust security mark on top of reasonable basis to encourage business investment and reinforcement of information security.	Ministry of Justice	The civil indemnification liabilities vary pending on individual cases and the degree of personal damage. Sentences are results of impartial judgment; legal systems should not interfere. The mark can be submitted as an evidence, which helps the judges to identify the scope of liability that should be laid on a business, that, the mark helps to reduce indemnification liabilities.
Organize national information security technology exchange/forum and competitions coordinated with incentives (monetary award, job opportunity)	Ministry of Economic Affairs	E-commerce Trust Security Talents and Stores Competition has been planned to upgrade the society's knowledge in trust security related issues. Develop e-commerce trust security human resources to create career opportunities.
Japan has a full set of plans when launching P-Mark; we should take the overall readiness of the industry environment into consideration when taking reference from the P-Mark system. I suggest that we should continue from the past experience of implementing ISO.	Ministry of Economic Affairs	Planning of the system will be based on the goal of constructing a full and comprehensive management system, including coordination with the nation's legal system and practical implementation needs in the industry. The goal of personal information management system is different from that of ISO (please see the appendix); nonetheless, it is still taken into reference.