Information and Communication Security Policy and Industrial Development Status of Main Countries

Dr. YAU JR LIU

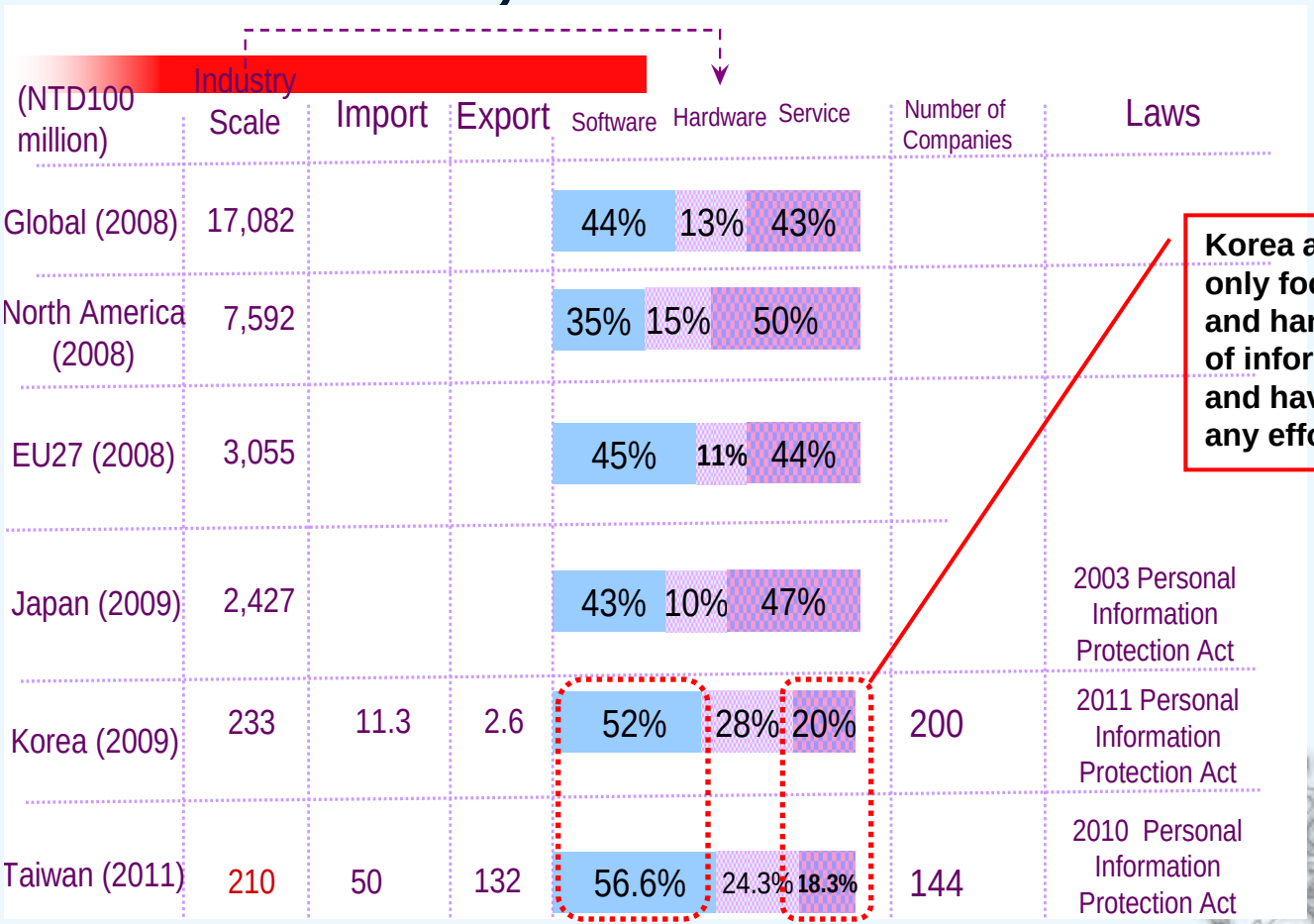
Outline

I Structure of the information security industry of main countries.

II Information security industry and policy of main countries

III Development of the information security industry in Taiwan

Structure of the information security industry of main countries



Source: IDC, JNSA Project “2008 Information Security Market Survey Report”, KISA (2009), Institute for Information Security “Information Service Industry Yearbook” 2011, TIER 2010 Survey Research.

Information security industry and policy of main countries

- **Information security industry and policy of the U.S.**
- **Information security industry and policy of Japan**
- **Information security industry and policy of Korea**

Current Status of Information Security – 2011 Internet Crime Report (1/6)

Source: IC3, “2011 Internet Crime Report”

◆The Internet Crime Complaint Center (IC3) issued the “2011 Internet Crime Report” in May 2012. The report showed that the IC3 received 314,246 reports in 2011, a 3.4% increase compared with the 303,809 reports in 2010, but a 6.5% decrease compared with the reports in 2009; over 300 thousand reports had been reported for three consecutive years.

◆The most common crime types include: FBI-related scams , identity theft, advance fee fraud, non-auction-non-delivery of merchandise, and overpayment fraud. More and more people are become victims of internet crime, and losses have reached US$485.3 million.

U.S. – Background of the Information Security Industry Policy (2/6)

2011 Action Strategy for Cyberspace

(1) Establishment of **USSTRATCOM** in response to complex challenges in cyberspace

① **Increase training** to ensure information security, increase sensitivity to incidents, and control risk;

② **Build smart partnerships**, establish collective self-defense to ensure the integrity and availability of cyberspace;

③ **Closely collaborate with operations commands, service providers and institutions,** and rapidly develop general capacity for innovative technologies.

(2) Change cyberspace defense concepts to form **active dynamic defense** of DoD network and systems.

① Step up network defense, employee communications management and internal control.

② Active network defense measures.

(3) Step up collaborations with other government departments and institutions, such as the Department of Homeland Security and Defense Industrial Base, search for **new collaboration methods with the private sector**, and strengthen network security measures for infrastructure with important military value, e.g. **power grid, financial industry and transportation systems.**

(4) Intensify **international collaborations**, jointly develop **sharable warning functions**, and adopt joint training activities to establish "network collective defense."

(5) Drive science, academic and economic resource utilization in the U.S., and establish a **network technical personnel and military personnel training center.**

U.S. – Laws and Regulations (3/6)

1992 computer security training policy

1998 important infrastructure protection

2001 president manage-ment manual

2002 national security bill Electronic government act

2003 national internet security strategy

2004 anti-spam act

Protect America Act of 2007

FISA Amendments Act of 2008

2010 Department of Homeland Security Appropriations Act (dedicated funds for information security – including cloud security)

2011 Foreign Intelligence Surveillance Act

~1998 1999 2000 2001 2002 2003 2004 2007 2008 2009 2010 2011

1999 Federal information security automation

2000 Global and national commerce act

2008 NSPD-54 Authorization NSA, CIA and FBI joint monitoring and detection of federal agency network

Legislation to dedicate funds for infrastructure protection and information security plans and activities

CyberSecurity Legislative Proposal

Computer security, e-commerce security ← 911 Incident → National security, passive defense ← Active preventive investigation → Cloud technology data protection

Source: Law Libraries of Congress and the House of Representatives, OMB

U.S. – Industrial Technology R&D (4/6)

1. Institution integration

2. Strategic framework for network and information technology research and development (NITRD)

Focus on changing planning and systems for technology R&D in the information security industry, develop the existing network and information technology research, develop strategies and other R&D related matters, in which **CSIA (Cyber Security and Information Assurance)** is responsible for information security R&D in NITRD.

- Implementation directions:

(a) Moving Target: Information Security Automation Program (ISAP)

(b) Tailored Trustworthy Spaces

(c) Cyber Economic Incentives

3. Coordination of the industrial sector and academic research

Coordination of the industrial sector and academic research to prevent repeated research; enable the industrial sector and academic research to be synchronized and complement each other, ensure that technology can be commercialized and enters the market.

4. Stronger collaboration between the federal government and industrial sector, for instance, establishing an in formation security laboratory

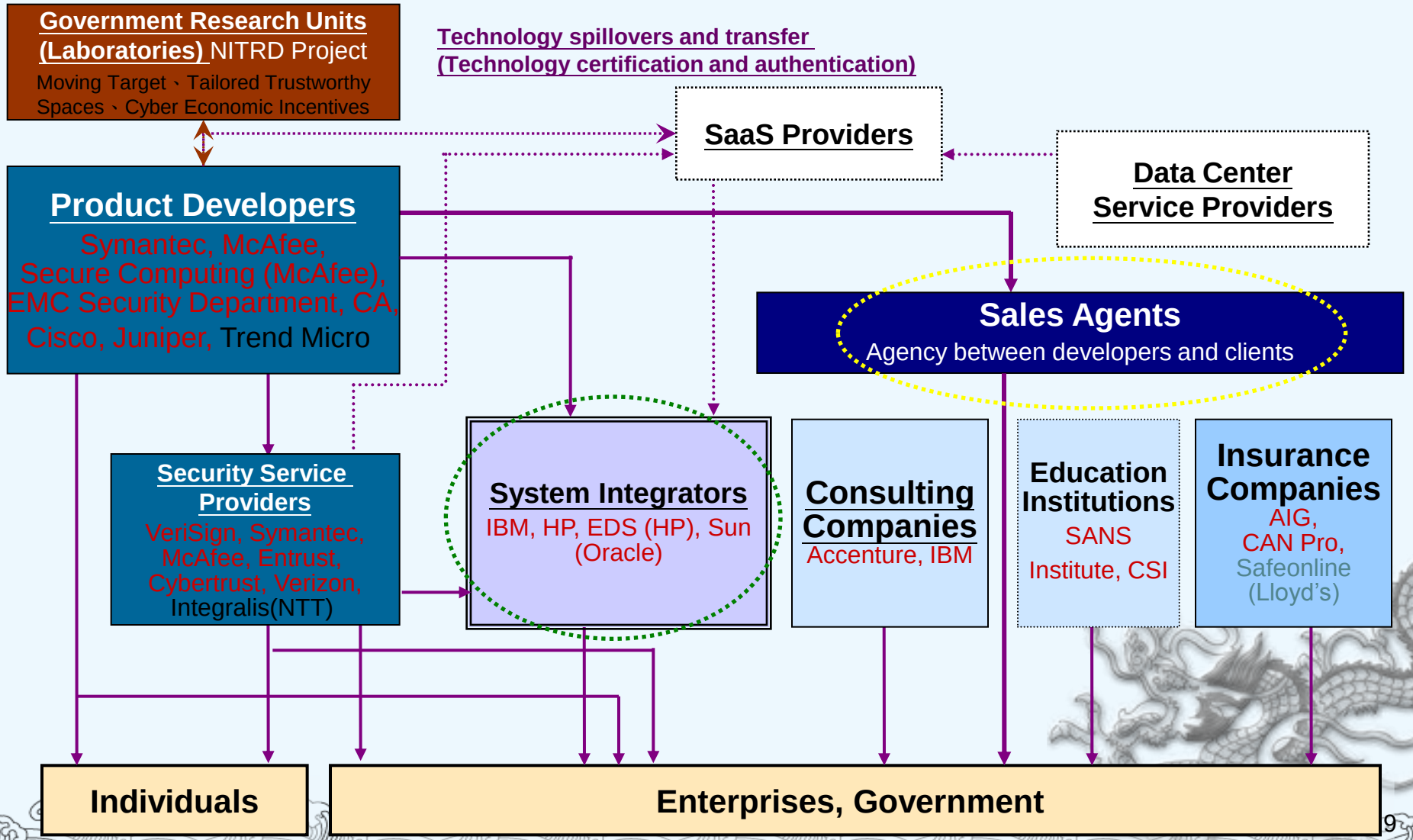
To strengthen the competitiveness of the U.S., the federal government is strengthening collaborations with the industrial sector, implementing industrial development and incentive measures, and rapidly approving research and technology development, including encouraging collaborative laboratories between academia and the industrial sector.

5. Joint establishment of design platforms and standards for information security by the federal government and industrial sector

The federal government should jointly establish infrastructure objectives and R&D framework with the private sector and other stakeholders, so as to verify objectives and establish national and international standards.

Source: Strategic framework for NITRD, NITRD Supplement to the President's FY 2012 Budget, organized by TIER

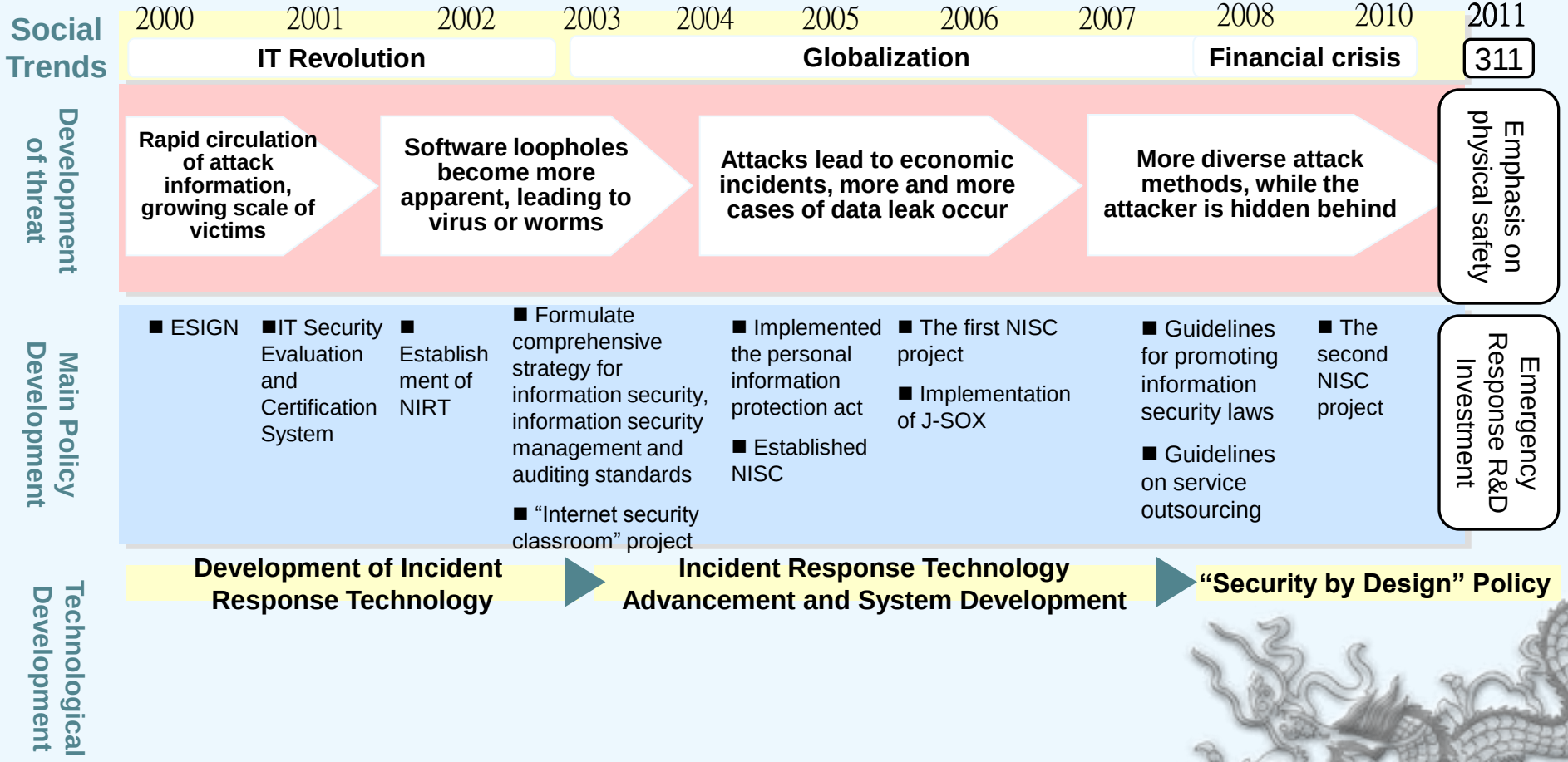
U.S. – Information Security Industrial Chain Structure (5/6)



SWOT Analysis of U.S. Information Security (Industry) Policy (6/6)

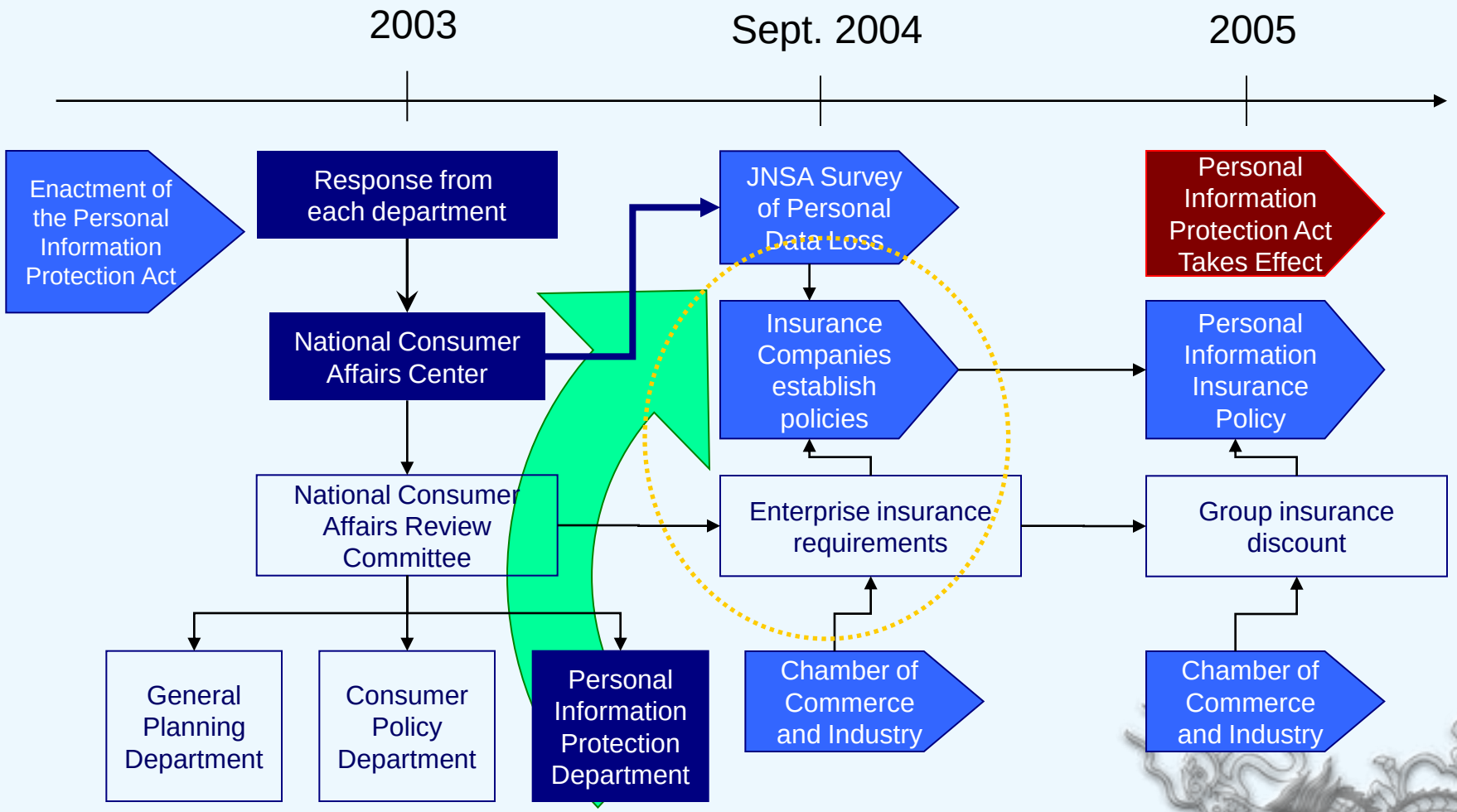
	Opportunities	Threats
Strengths	**SO :** 1. Government investment in information security R&D is the highest in the world. 2. Strong platform operators and information security firms will further expand the industry under developments of cloud technology.	**ST :** 1. Emphasis on response capability of personnel (e.g. Cyber Storm), overall output value of the information service industry will increase under government guidance. 2.Internet and Information Innovation Sector (I3S) policy will increase the use of American information security products in the domestic market, preventing the threat of foreign products entering the market.
Weaknesses	**WO :** Decreasing funding for information security, R&D policy focuses on developing priority and incentivized items.	**WT :** Outflow of technology talent in the field of information security; the 2011 Action Strategy for Cyberspace establishes an internet technical personnel and military personnel training center for talent cultivation.

Japan – Industrial Development Policy (1/6)



Source: JNSA Project "2008 Information Security Market Survey Report," Organized by TIER.

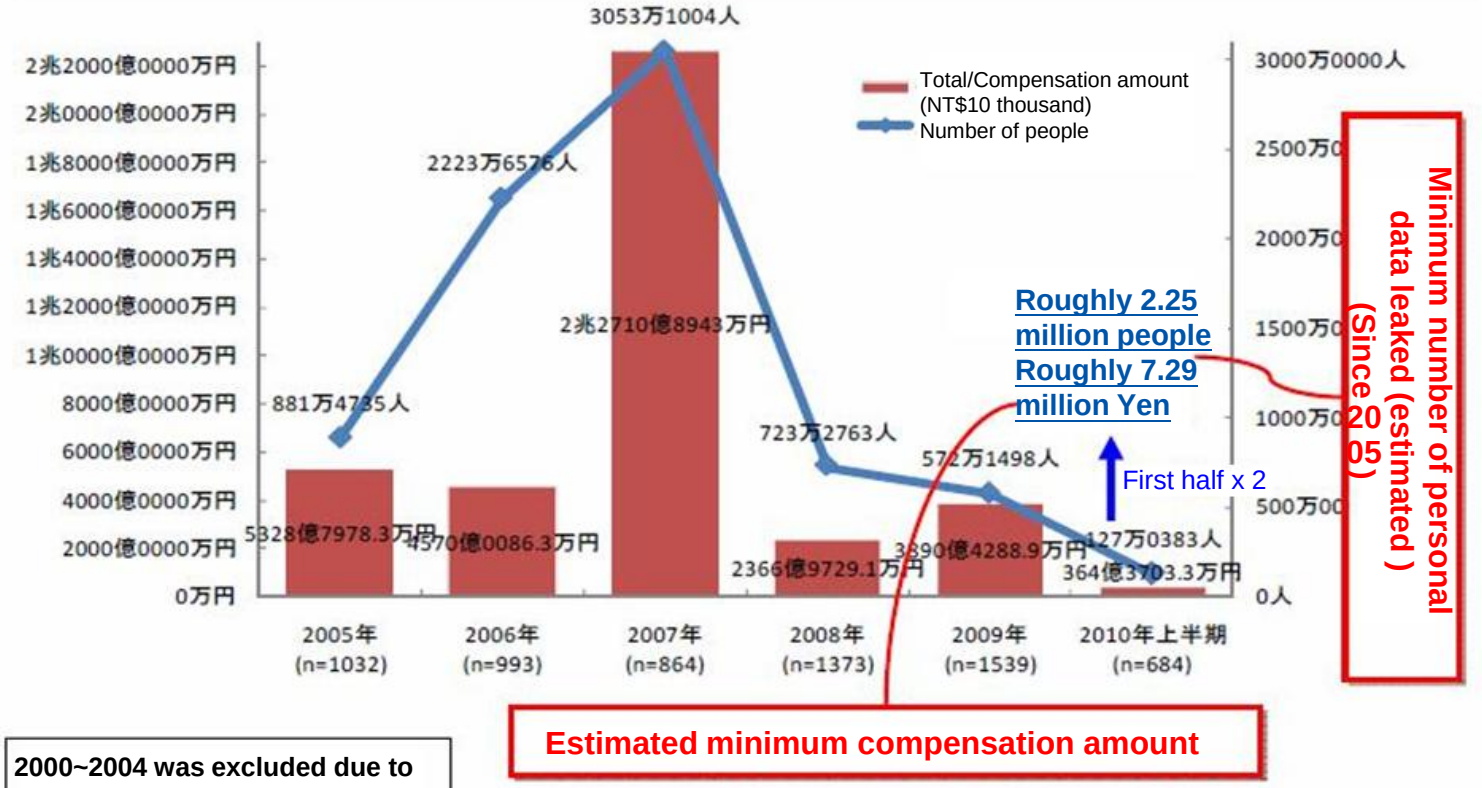
Japan – Personal Information Insurance (2/6)



Source: Chamber of Commerce and Industry, Japan, organized by the TIER.

Japan – JNSA Investigation (3/6)

Number of Personal Data Leaked and Compensation Amount (2005~2010)

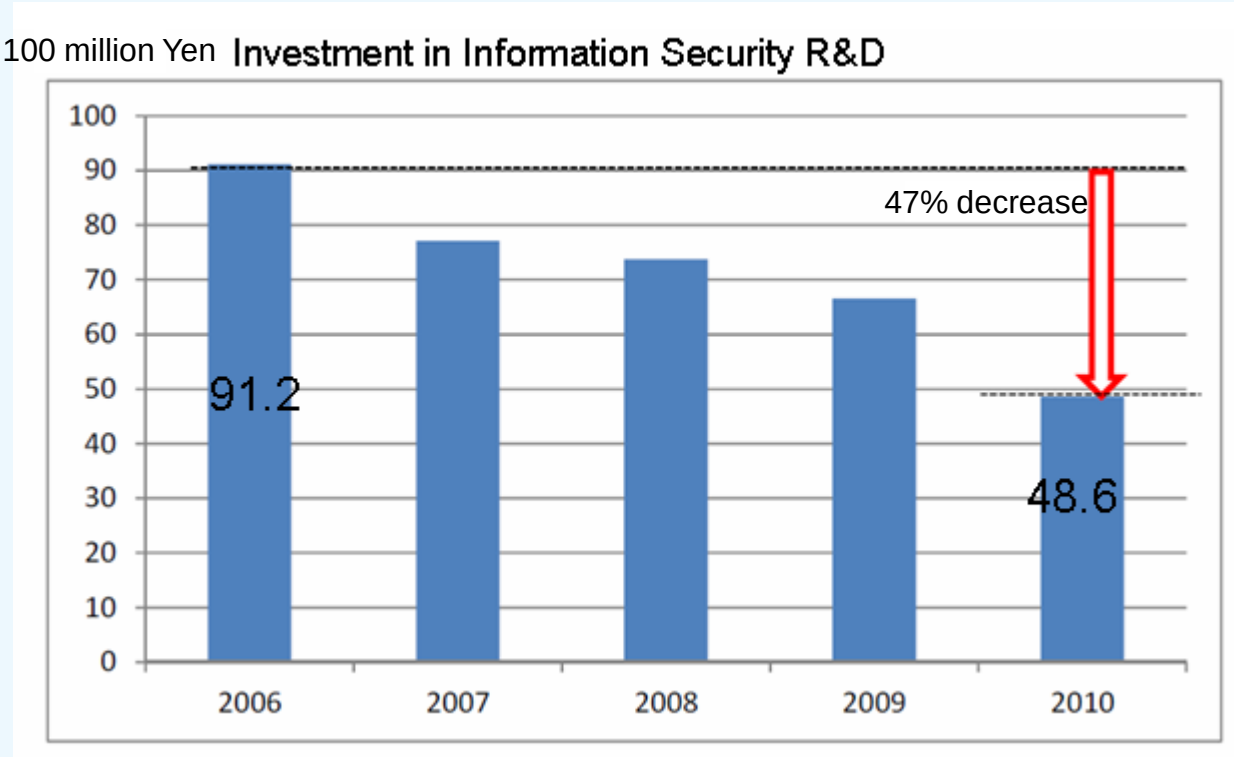


Source: 2000-2011 NPO Japan Network Security Association

◆**2010 Actual data leak in 2010 resulted in loss of 121,576,000,000 Yen**
(Data leak in schools and financial institutions are mainly via e-mail and FAX)

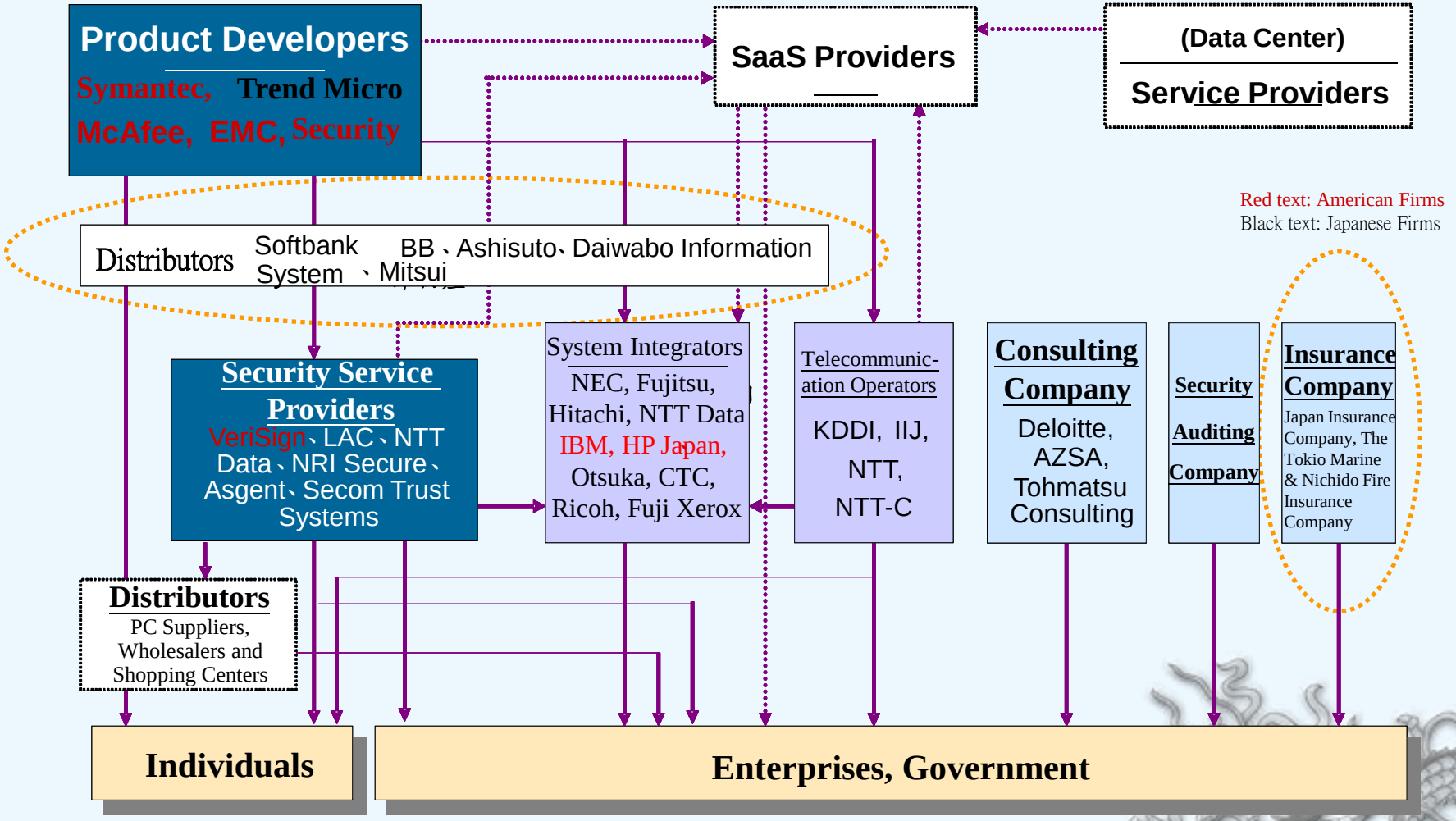
Japan – Investment in Information Security R&D (4/6)

- **Key points of the 2011 Information Security R&D Strategy**
  1. Active and highly reliable information security
  2. Improve the security of emergency response systems, develop a high disaster-resistant information reporting system from the perspective of information security, and R&D “risk management” and “risk intelligence.”
  3. Expand R&D to globalize the information security industry.



Source: July 8th, 2011 Information Security R&D Strategy, Information Security Policy Meeting

Japan – Information Security Industrial Chain Structure (5/6)

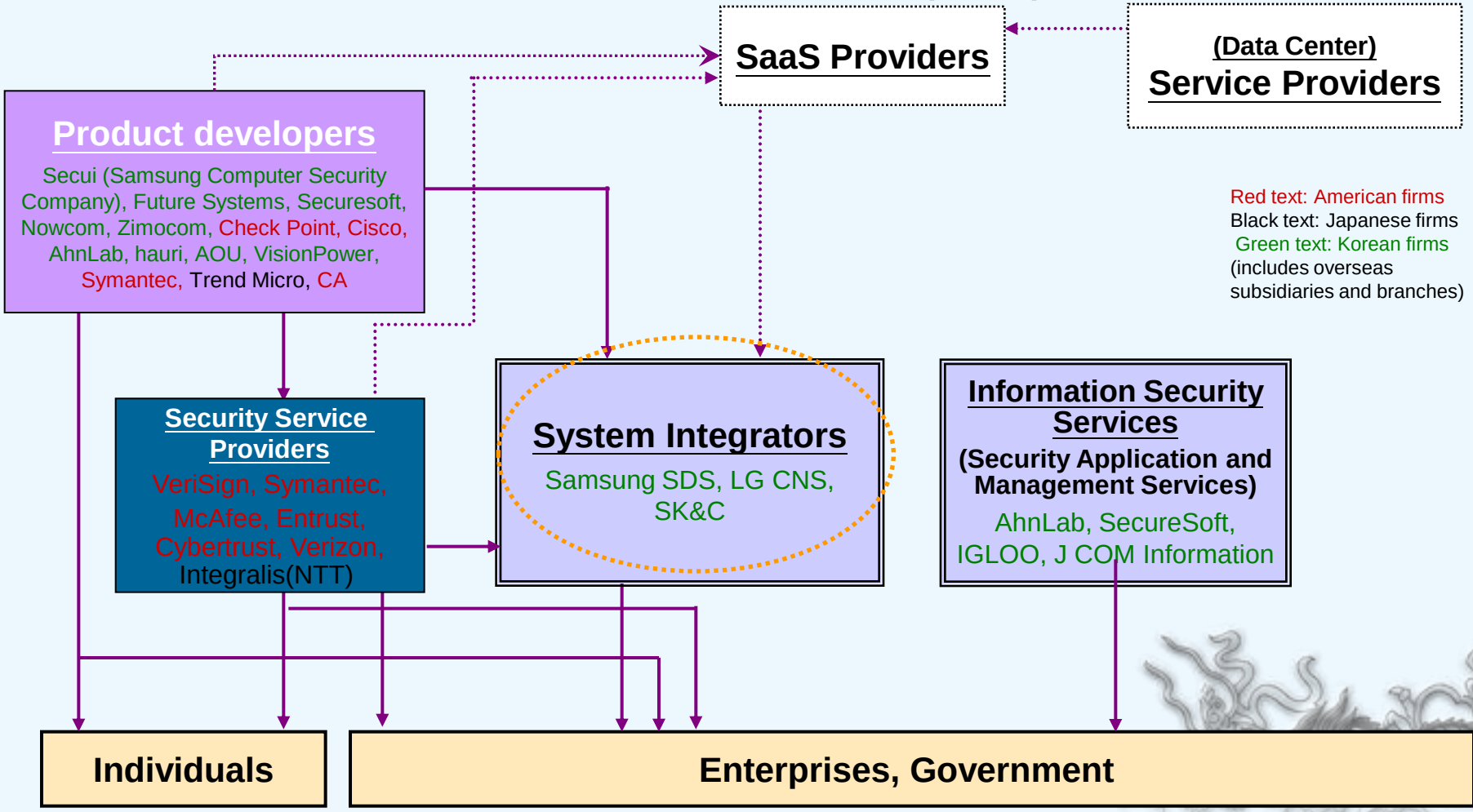


Source: Categories defined in the "2008 Information Security Market Survey Report" of JNSA

SWOT Analysis of Japan Information Security (Industry) Policy (6/6)

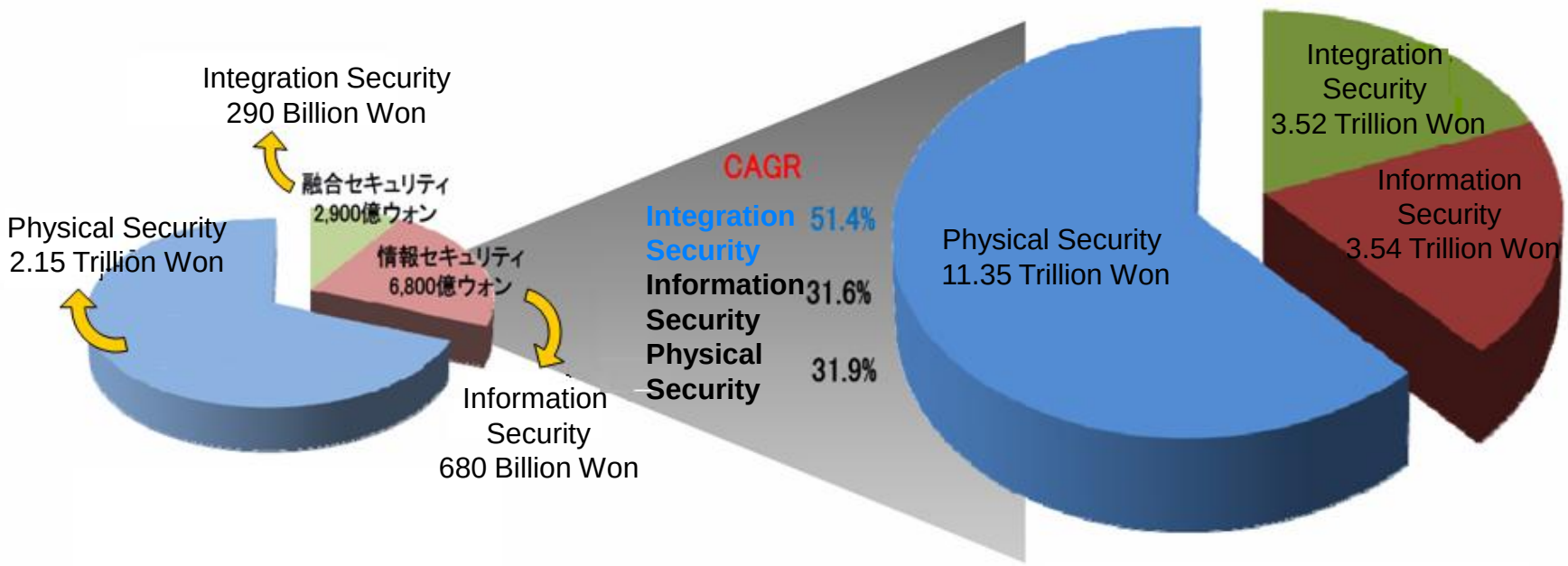
	Opportunities	Threats
Strengths	**SO :** Following development towards virtual and cloud technology, system security management products will become more and more important; Japan currently has an advantage in the product, coupled with growing attention from the government, the information security industry will have even more development opportunities.	**ST :** Japan has an immense domestic information security market (14.2% of the global market). After the Personal Information Protection Act was enacted, collaborating with Japanese distributors and suppliers is the key for foreign suppliers to enter Japan's market.
Weaknesses	**WO :** 1. After the 311 earthquake, Japan enhanced the security of its emergency response system, developed a highly disaster-resistant information reporting system with consideration to information security, and focused on R&D of "risk management" and "risk intelligence"; information security products are developing from virtual towards physical. 2. The Personal Information Insurance System has not only increased information security protection for enterprises, but also driven development of the information security industry.	**WT :** With significantly less funding for information security R&D, research capabilities of the private sector will become growingly important; an information security expert cultivation system is implemented to strengthen information security R&D capabilities of the private sector.

South Korea – Information Security Industrial Chain Structure (1/5)



South Korea – Outlooks for the Knowledge and Information Security Market (4/5)

◆**The knowledge and information security market will reach 18 trillion KRW in 2013**



2007 (3.12 trillion Won)
(NT$104 billion)

2013 (E) (18.4 trillion Won)
(NT$613 billion)

Source: 2009 Domestic Knowledge and Information Security Market Survey, KISA (brief of KISA given in Japan for NPO and related agencies)

South Korea – Information Security and Industry Integration Model (4/5)

Cultivation of the next generation growth engine: "10 IT Industry Integration Strategy"

Utilization of the mature IT industry to integrate information technology and products and increase the competitiveness of traditional industrial; rise of an IT integration model
=>Integration of IT and other industries to drive the development of new services and products

South Korea's future IT strategy (200909):

◆**The 10 IT Industry Integration Strategy focuses on driving industrial development and expanding overspills**

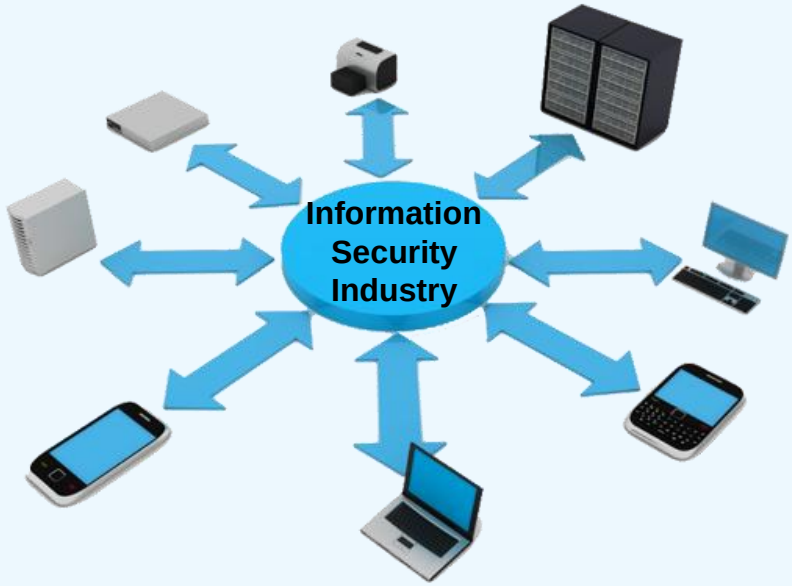
◆**Expand IT integration technology via investment in R&D, establish an integration information technology center, establish a Green IT national strategy**

SWOT Analysis of Korean Information Security (Industry) Policy (5/5)

	Opportunities	Threats
Strengths	**SO :** As the government is promoting the concept of industry integration security, the information security industry will grow along with the prosperous development of the ICT industry, becoming an indispensable satellite industry of the ICT industry.	**ST :** Sequential increase of information security patents each year shows that Korean information security firms are growing along with demand of other ICT industries.
Weaknesses	**WO :** Implementation of the Personal Information Protection Act will benefit the information security service industry to a certain extent.	**WT :** Government information security R&D capacity is mainly held by KISA, most items cohere with industry and commercial trade security; under the policy to integrate knowledge and information security industries, industrial demand should drive development of the information security industry.

Status of the Information Security Industry in Taiwan

- **Development status of the information security industry in Taiwan**
- **Demand of the information security industry**



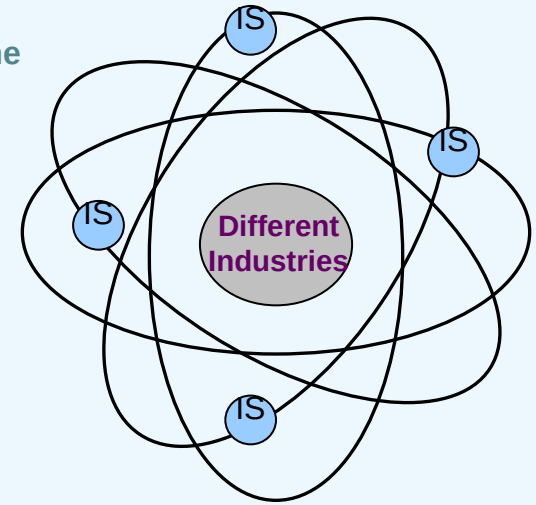
Development Status of the Information Security Industry in Taiwan

South Korea's Information Security Industry Strategy

(Integration policy for the knowledge security industry)

❖Online Game

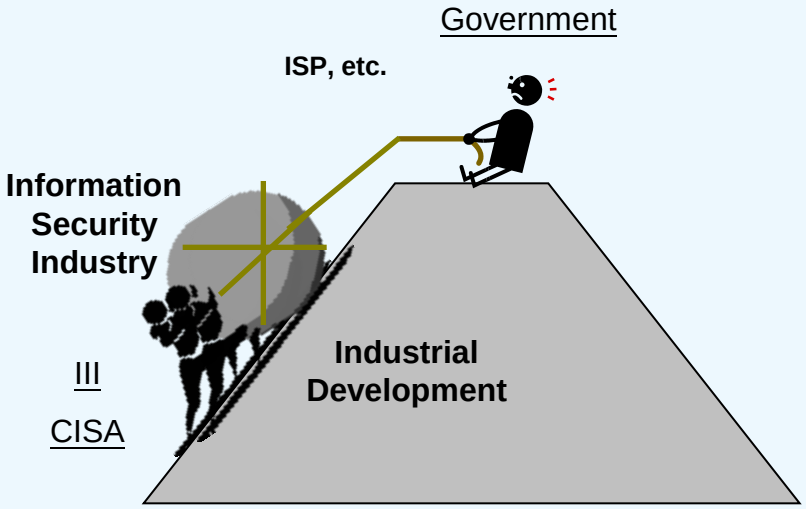
❖ICT devices



- ✓Smart grid and information security integration
- ✓Mandate the gaming industry use information security software
- ✓Information security industry driven by large enterprises (e.g. Samsung)
- ✓Rapid development of information security patents

●South Korea's information security industry is relatively small, same as Taiwan, and focuses on software development. According to observations of this study, the industry satisfies demands of regular firms and other information industries (government utilization accounted for 30% in 2009).

Development status of the information security industry in Taiwan



- ✓Relatively weak software application industry
- ✓Insufficient support from large enterprises (only Trend Micro Taiwan)
- ✓Slow development of information security patents

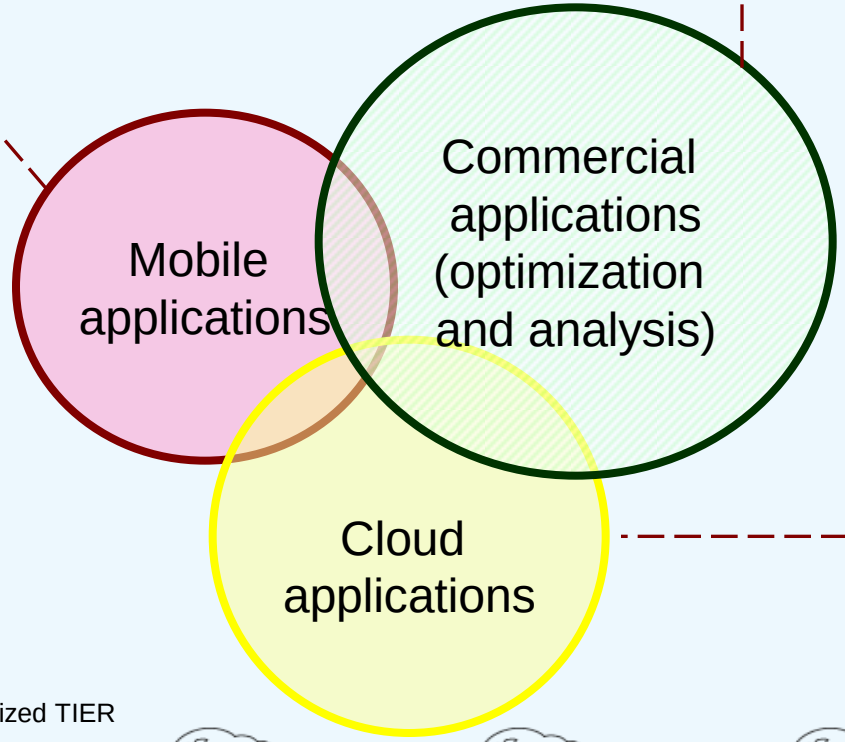
●Taiwan's information security industry is relatively small, mainly consisting of SMEs and aims to satisfy demands of regular firms

New Demand Brought by the Information Security Industry

Mobile Phone Protection

Information Security Integration Requirements

- ✓**New forms of prevention and defense （EX：Advanced Persistent Threats, APT）**
- ✓**Personal information control**
- ✓**Technology output for integration with industrial applications**
- ✓**Electronic medical record application**
- ✓**Personal information protection act and digital forensics**
- ✓**Secure erasing technology**
- ✓**E-discovery process**
- ✓**Social network spam reaching whole new levels**

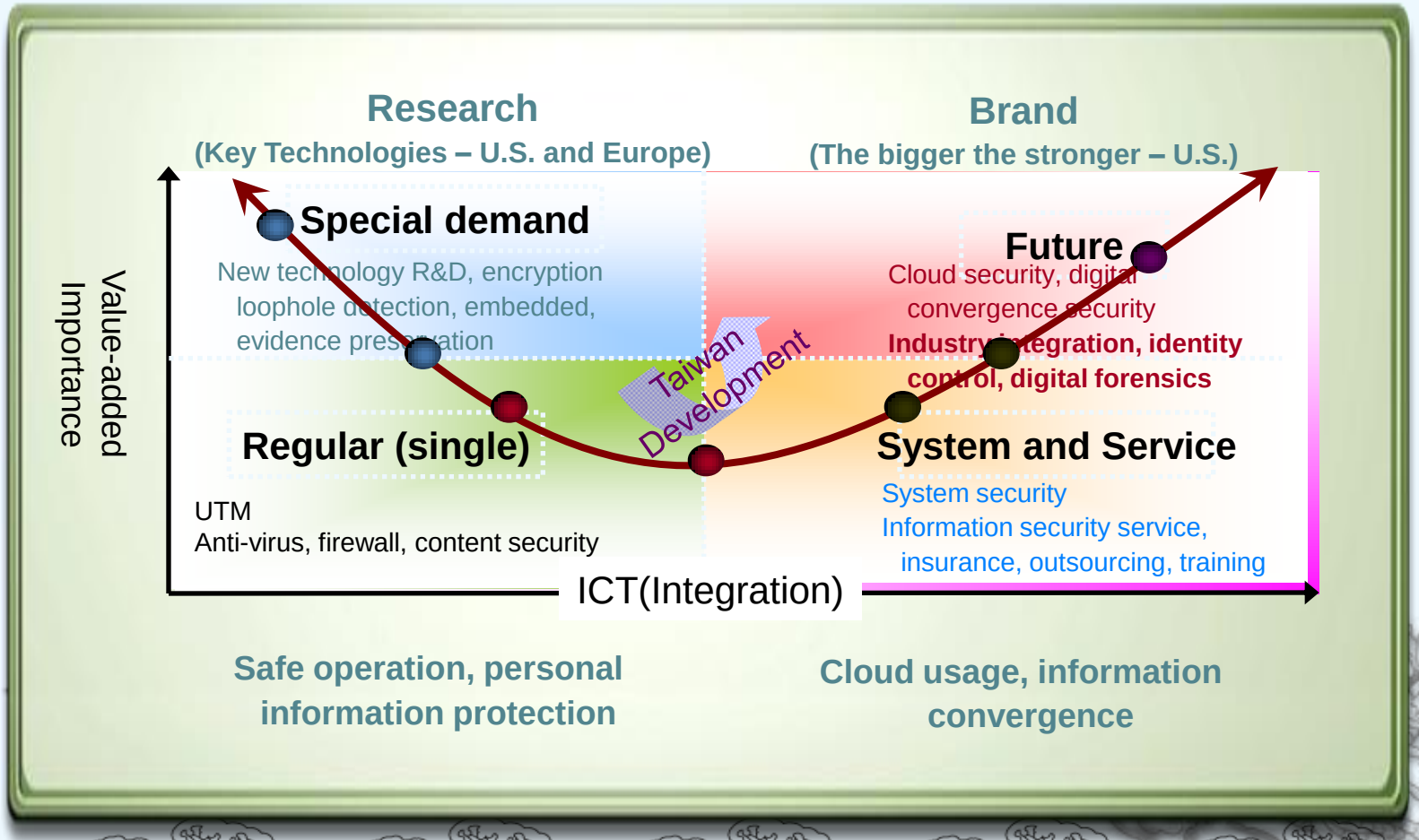


Cloud demand

Source: Organized TIER

Conclusions

- Value chains of the information security industry in each country (key technologies and products are controlled by multinational enterprises)
- Taiwan should mainly develop information security services in response to new demand (cloud, digital forensics, etc.)



科学技術振興機構
Japan Science and Technology Agency

行政院國家科學委員會
National Science Council

Thank You.