Topic 3: Facilitating the Development of Taiwan ICT Security Industry

August 19, 2009

Outline

I. Introduction

II. Global ICT Security Trends

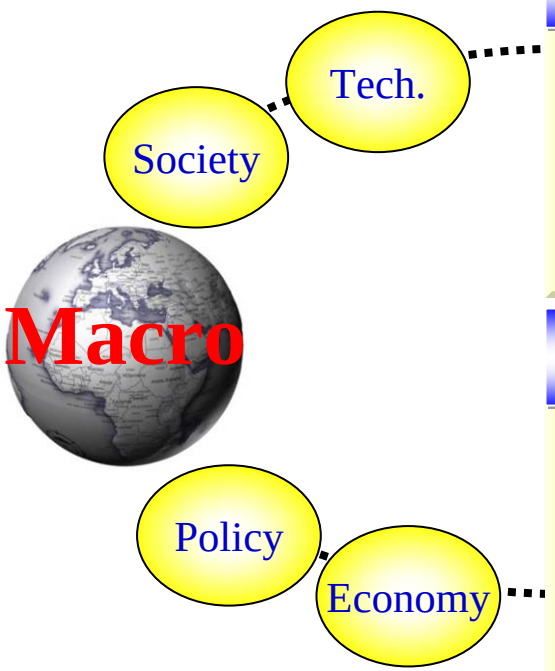
III. Current Status in Taiwan

IV. Development Strategies and Action Plans

V. Discussion Topics

I. Introduction

Expanding Impact of Security Incidents



Financial Transaction

Commercial transactions and related activities have increasingly relied on ICT technologies. With the widespread adoption of e-commerce, the general publics is conducting online transactions more and more frequently and in greater volume. It has been attracted potential cyberspace criminals' attentions.

Tech. & National Defense

A robust and comprehensive ICT capability is required for defending against the threat posed by international hackers to national security and government secrets. This will ensure national security, strengthen the security image of the nation, and support technology development.

Business Operation

ICT technologies have been extensively leveraged to manage all kinds of commercial, confidential and personal data for production procedures, customer information, logistics et al that will boost productivity and reduce costs.

Public Protection

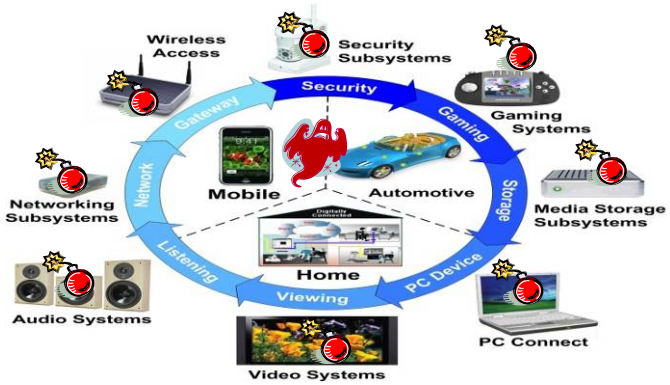
Most of the ICT cyber attacks are for financial or revengeful purpose. The attack approaches have become far more difficult to detect than before. Given the fast spread of malware and the lack of ICT security awareness in general publics, we can say that the public protection in cyber space is inadequate at present time.

- **McAfee research indicates that sensitive data leaking has caused over US$ 1 trillion losses in 2008.**
- **Consumer Report reveals a statistics that consumers suffered US$ 8.5 billion losses due to computer viruses/spyware from 2006 to 2008.**
- **Gartner shows that phishing attacks caused US$ 3.2 billion losses throughout the United States in 2007.**
- **In May 2007, the world's first Cyberwar took place in Estonia. The country's websites have been under heavy attack and almost paralyzed for one month due to the probable attacks from Russia.**
- **Taiwan Institute of Economic Research estimated that around 8% of the enterprises in Taiwan had lost up to NT$ 9.553 billion in 2007 because of ICT security events.**

Cyber Security Challenges in Digital Evolution

Trend 1: Increase in potential ICT security concerns from digital convergence and cloud computing services

- Digital convergence – Ease for malicious attack proliferation
- Cloud computing services – Ease of hiding for hackers

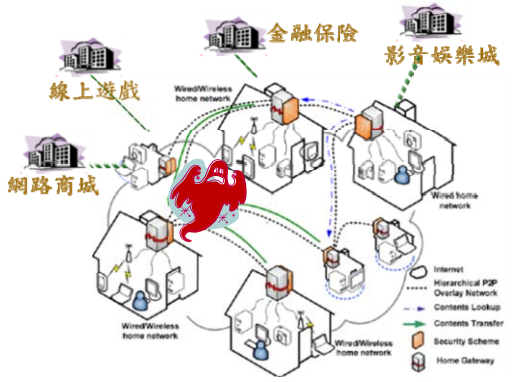


Trend 2: New ICT security issues due to the emerging of smart mobile applications

- Multiple platform integration – Disclose the vulnerabilities of ICT security
- Increase in mobile commerce applications – Become new attacking targets

Trend 3: ICT security threats because of the popularity of digital life at home

- Telecommuting – Raise the security needs for stay-at-home workers
- Convenient lifestyle applications – Concerns on protecting personal data and privacy



II. Global ICT Security Trends

Driving Forces of Global Security Market

Global ICT Security Market

US $M

2009 Nokia mobile phone has a vulnerability that affects SMS functions

2008 Citigroup customer data leakage reveals the major DNS vulnerabilities

2005 Logic bomb disrupts supply of Medco medical products

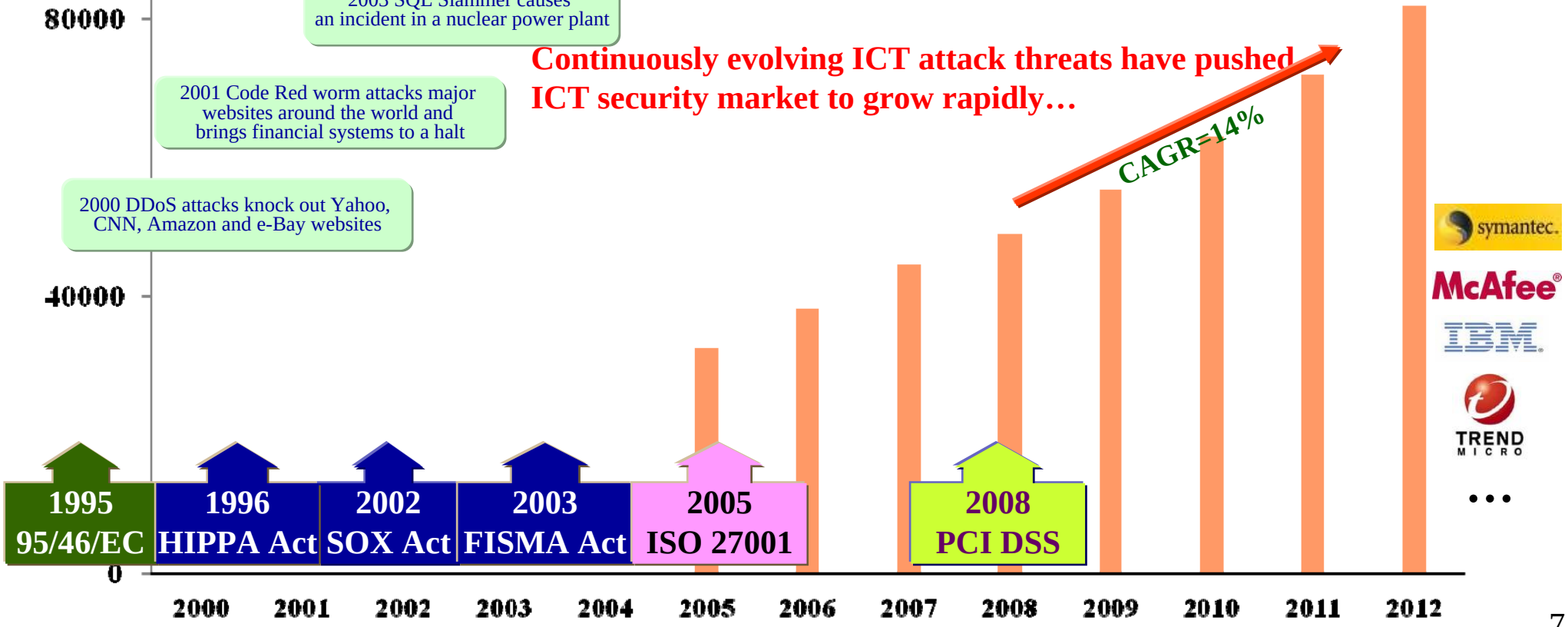
2003 SQL Slammer causes an incident in a nuclear power plant

2001 Code Red worm attacks major websites around the world and brings financial systems to a halt

2000 DDoS attacks knock out Yahoo, CNN, Amazon and e-Bay websites

ICT threats and regulatory requirements are spurring a rapid growth of the global market which volume is expected to be 81.8 billion USD in 2012

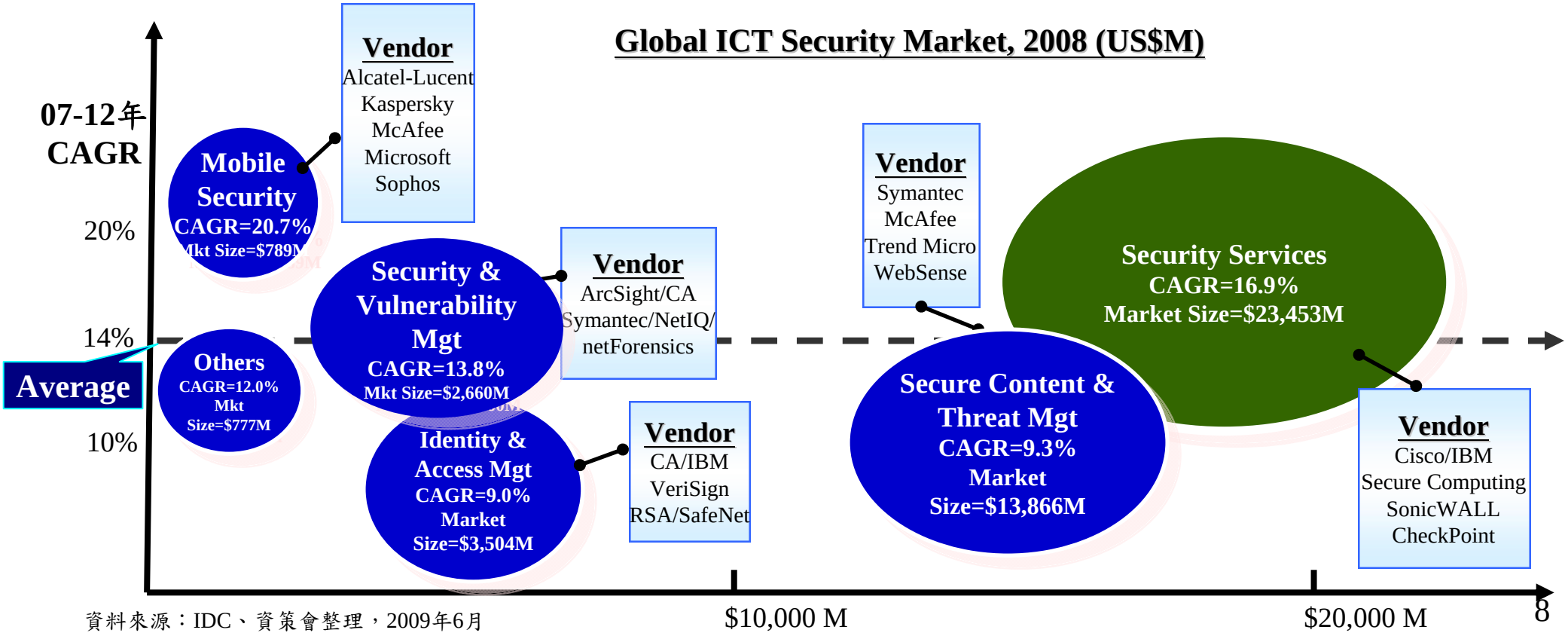
Continuously evolving ICT attack threats have pushed ICT security market to grow rapidly…



Source: Collated by the III IDC

Global Security Market Segments & Revenues

- **Among ICT security products, the secure content and threat management market is the largest sector. Mobile security has the highest growth rate (CAGR=20.7%), followed by vulnerability management. The potential in the market is significant for Taiwan ICT Security vendors to pay more attentions.**
- **Although the size of the ICT security services market is tremendous, vendors have to provide services by leveraging ICT security products.**

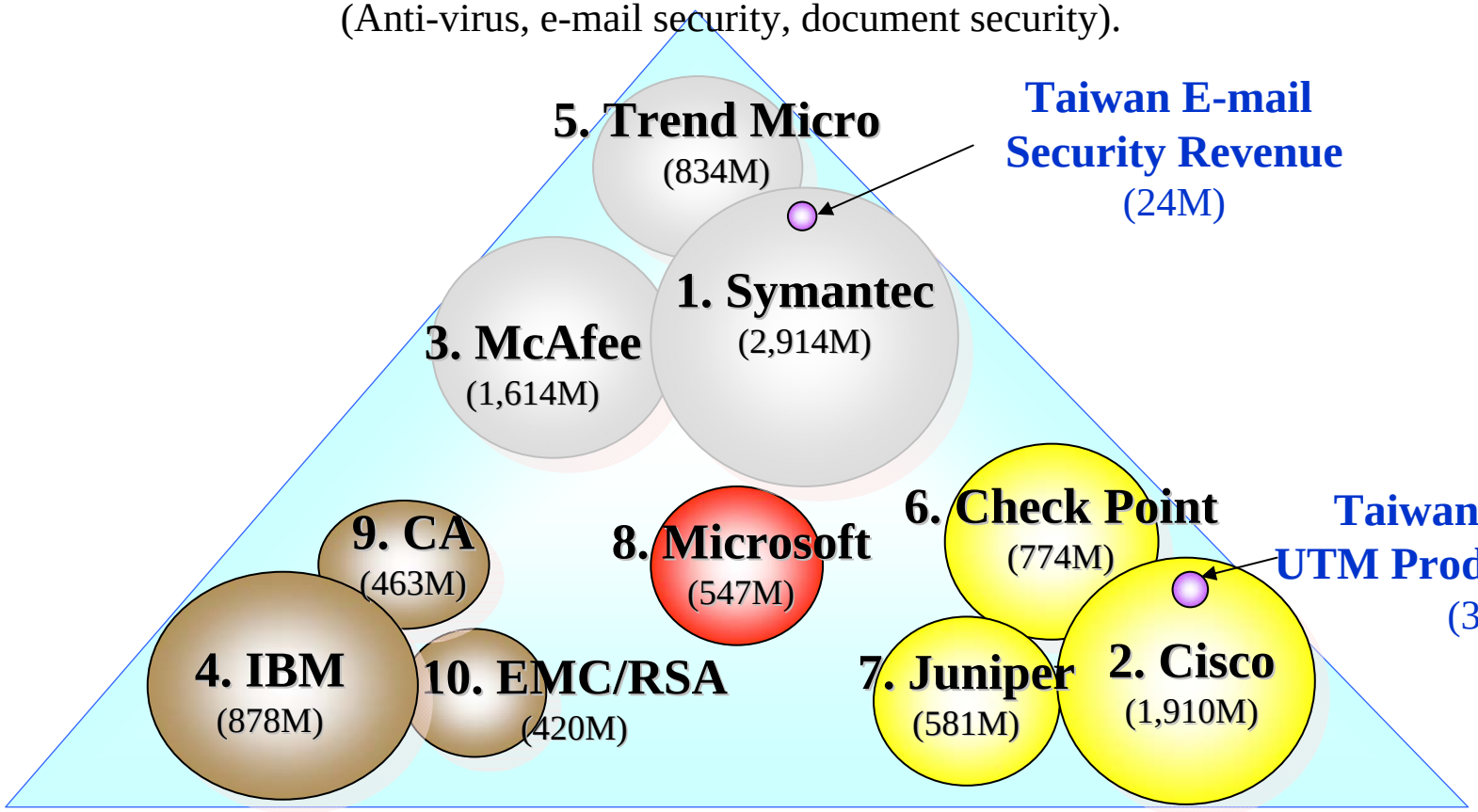


資料來源：IDC、資策會整理，2009年6月

Global Top 10 Vendors & Their Product Types

Secure Content

(Anti-virus, e-mail security, document security).



Identity / Vulnerability Mgt.

Threat Management

(Firewall, Intrusion detection, UTM)

Note: The size of each circle represents the relative volume of the vendor's revenue (in US$M). Each vendor's number is the rank of their market share in the global ICT security market.
Source: III MIC (June 2009).

ICT Security Trends with Digital Applications

資訊應用

Cloud Computing & Ubiquitous Service

Internet applications have entered the Web Service era. After moving to cloud and mobile computing services, more ICT security challenges have emerged…

Cloud Computing & Ubiquitous Service Security

Virtual Resources
Cloud Client Mash-up

Cloud App (XML/RIA) FW (威脅管理)
Proactive Malware Detection (內容安全)
Mobile Security/Privacy (威脅管理/內容安全)

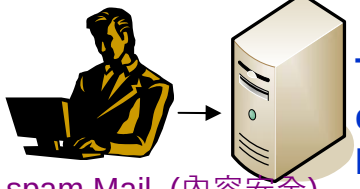
Web Service Security

Web Service

SOA, Blog,
Web-based Office..

Web App Firewall (威脅管理)
Web DB Security Monitor (威脅管理)
SIEM/Taint Analyzer (內容安全/ 弱點管理)

Inter-networking Security



Telnet/FTP/
e-Mail/
Browsing..

Internet service

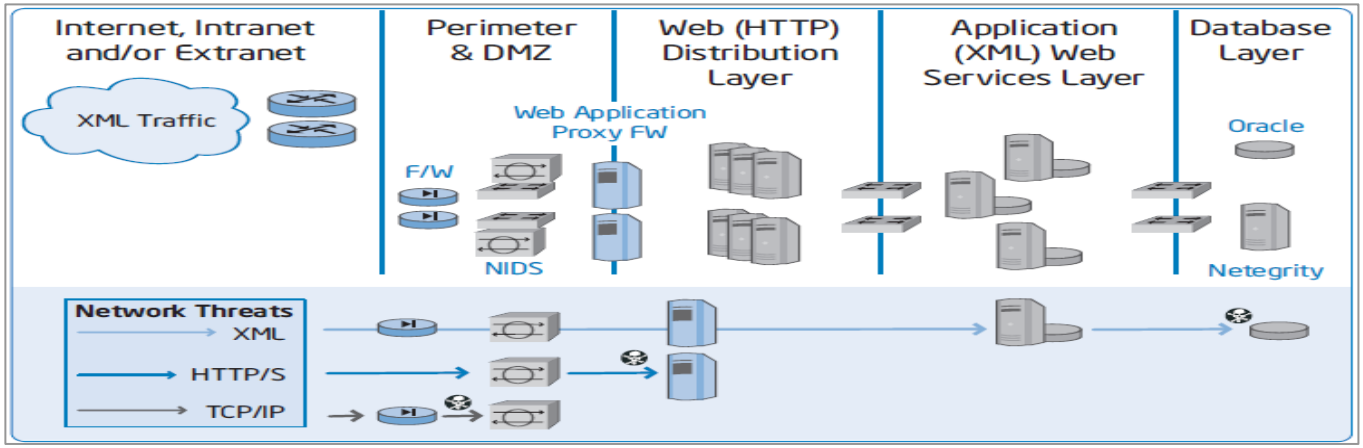
Anti-spam Mail, (內容安全)
VA, F/W, IDS, IPS (威脅管理)
PKI, VPN (身分辨識)

2005 **2010** **2015**

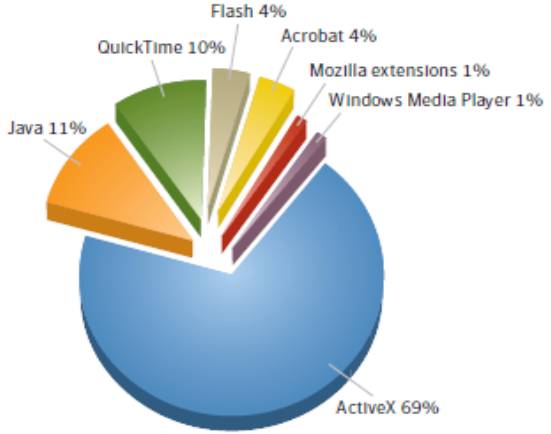
Web Attacks Driving Defense Technology

Over 70% of ICT security vulnerabilities are pertinent to web applications. Well-known websites (CNN, Business Week, McAfee) became relays for hackers after compromised

- The majority of application layer protection technologies are URL filtering techniques today. In addition, new attacks are targeting XML, Web DB and RIA (Rich Internet Applications, including Active-X, Acrobat, Flash, etc.).
- In response to the constantly-evolving challenges of Web security threats, this security market has grown rapidly (CAGR=13.7%).
- Trend in evolution of ICT security defenses:



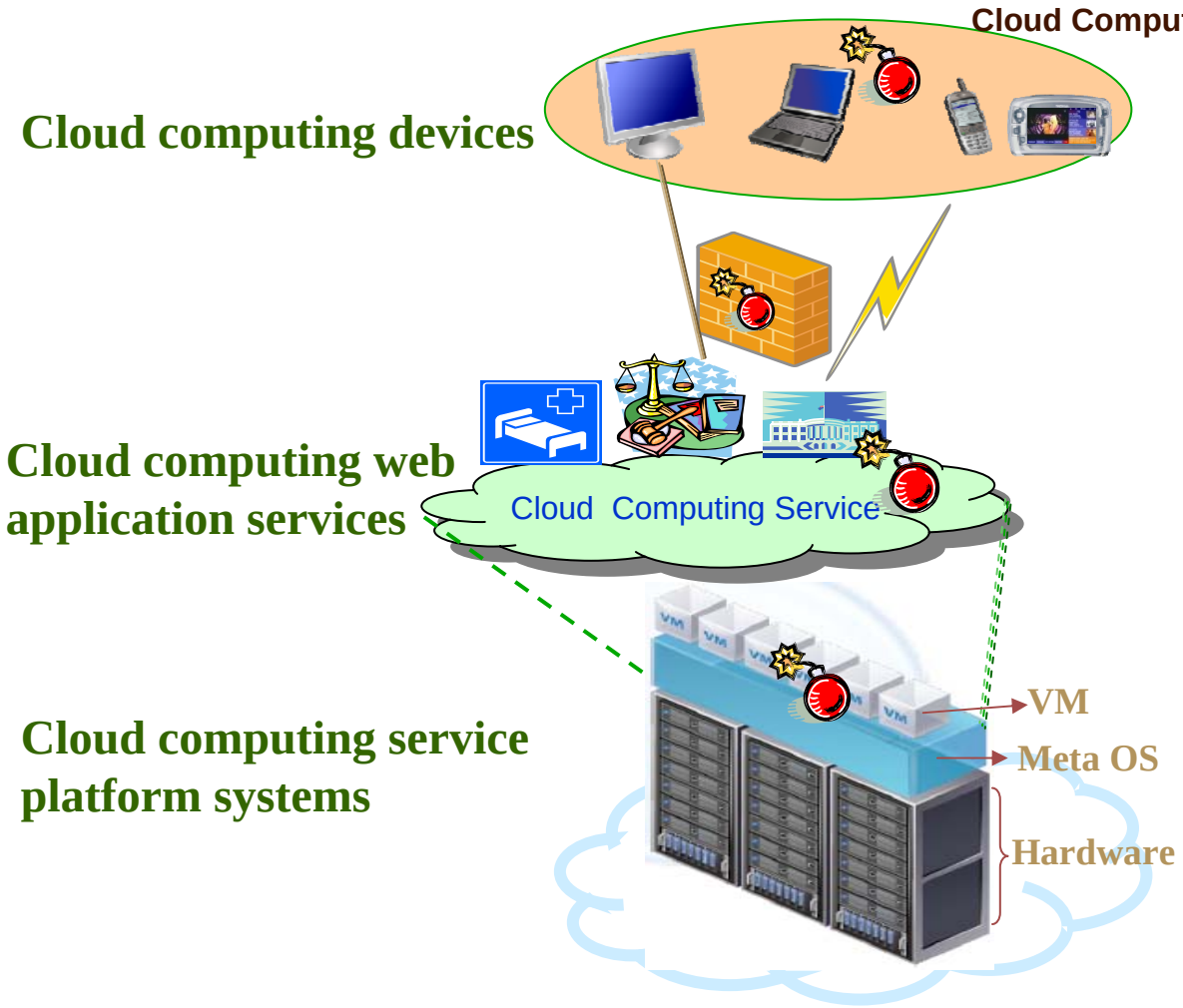
Network Layer Defenses. → Application Layer Defenses. → Web Service/DB Defenses..



RIA ICT security vulnerability ratio
Source: Symantec

Cloud Computing Security Overview

Cloud computing services are now considered to be the next major application trend in ICT industry following web services. The multi-layer technical architecture and dynamic computing infrastructure will face more ICT security threats that include cloud computing device security, web portal protection, cloud computing content access security, and cloud computing system vulnerability management.



- Cloud computing device security
- Web portal protection
- Cloud computing content access security
- Cloud computing system vulnerability management

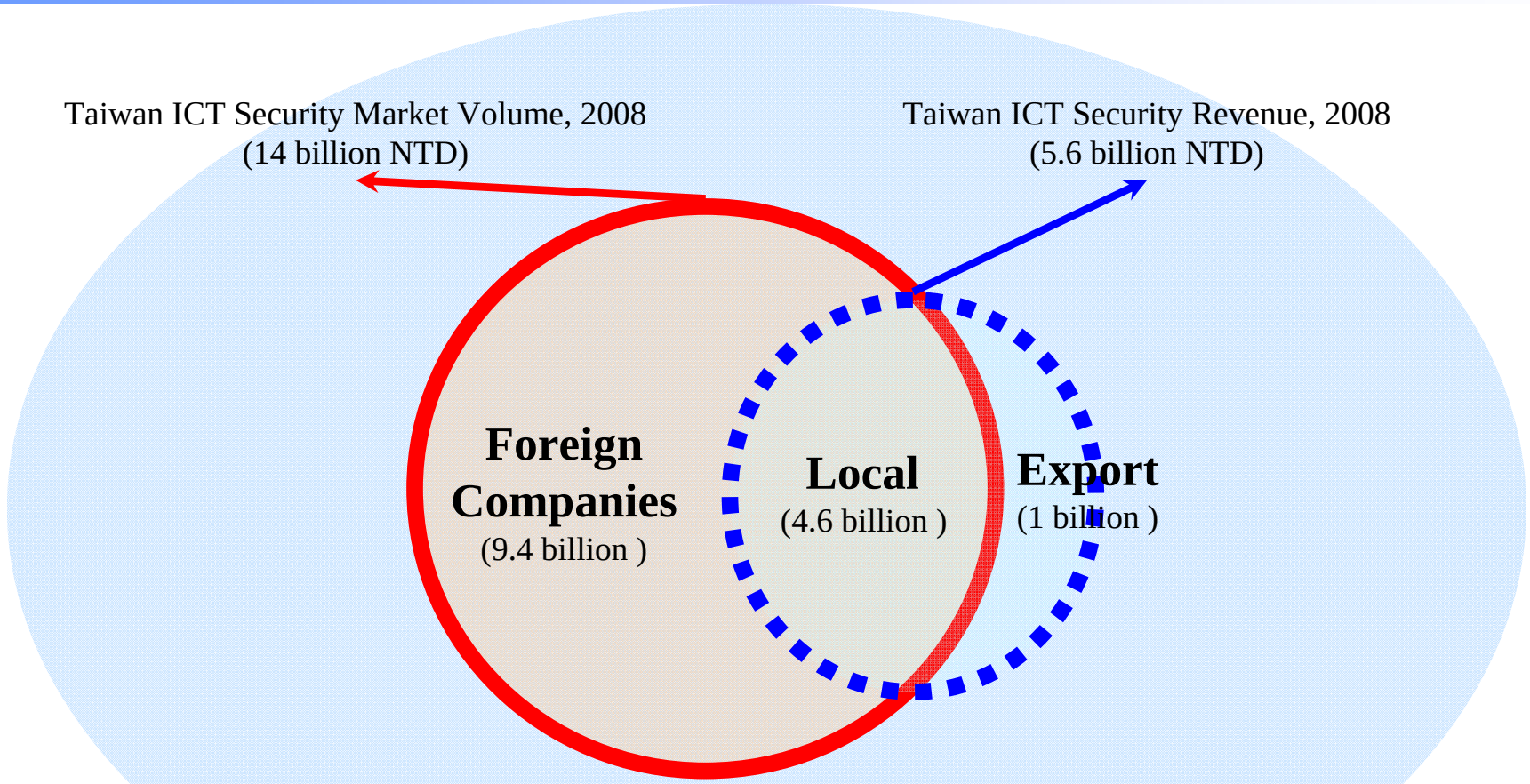
Cloud computing security issues

ICT Security Policies around the Globe

- US President Obama announced, on May 29, 2009, a new project to promote the network security in USA, which includes the appointment of a "Cyber Czar" at the White House responsible for coordinating all ICT security activities, deterring and preventing cybercrime and espionage against the US government-run and private computer networks, as well as dealing with hacker attacks.
- In March, 2004, the European Union established the European Network and Information Security Agency (ENISA) with an annual budget around € 20 ~ 35 billion.
- In 2001, Korea upgraded its ICT security research organization to higher level and named as the Korea Information Security Agency (KISA) whose responsibility is for developing ICT security technology and policy. Its mission is to realize the promise of a secure and dependable information society.
- Japan set up the ISEC department under its Information Promotion Agency (IPA) for facilitating the development of ICT technologies. These include the ICT security related projects, such as computer viruses, intrusion, and cryptography.
- In China, the State Information Center organized a Network Security Department in charge for information security development planning and strategic research, construction and management of large-scale security engineering projects, standardization of ICT security technology, ICT security brokering service, information resource development, and security technology services.

III. Current Status in Taiwan

Market Volume of Taiwan ICT Security

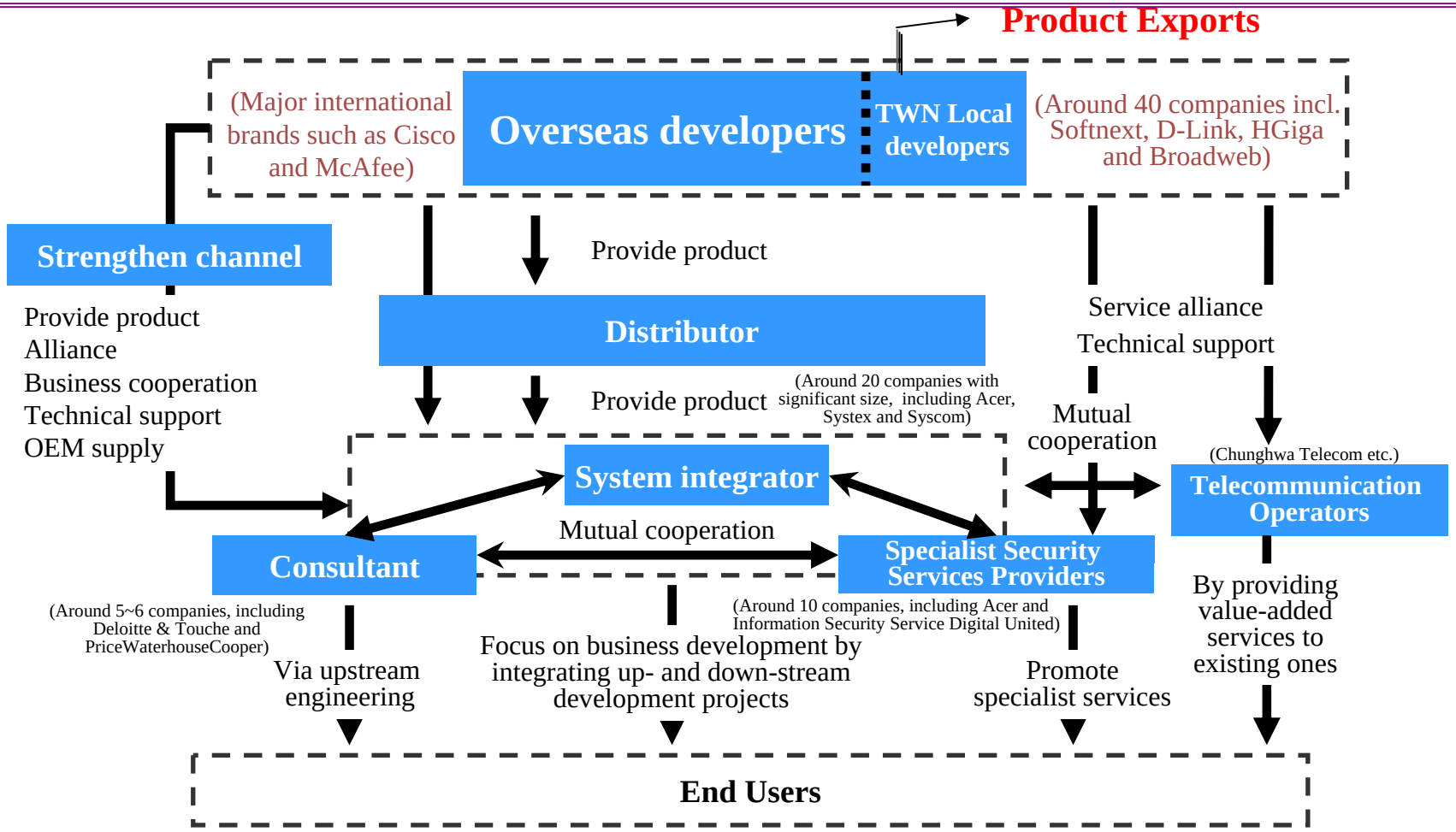


Other derivative ICT security related products' revenue is around 24 billion NTD.
(including network equipment with integrated ICT security such as the SOHO router and WLAN AP).

- **The Taiwan ICT security market volume (including products and services) is approximately NT$14 billion. Domestic vendors occupy 1/3 of the market share.**
- **The export by Taiwan ICT security vendors is around NT$ 1 billion. ICT security products include ICT security software and dedicated ICT security hardware (Firewall/UTM).**

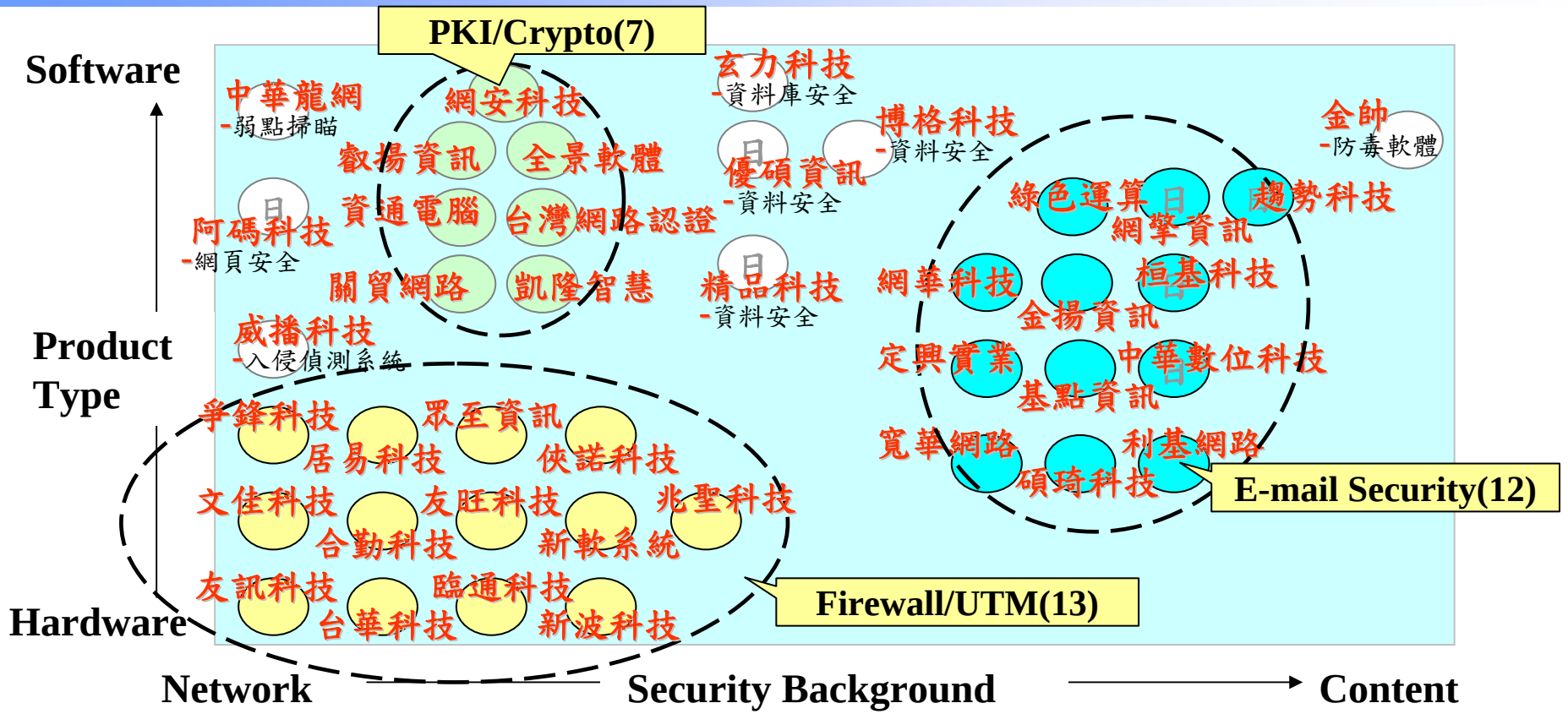
Ecosystem of ICT Security Market in Taiwan

The majority of the ICT security products used in the domestic market are imported from foreign countries. There are around 40 local vendors, but they only occupy a small portion of the market. The size of these domestic vendors is usually small. Hence, they usually lack the ability to make research and to exploit the international market.



Source: III MIC (November 2008).

Overview of Product Developers in Taiwan



- Taiwan ICT security industry is developed based on the unique advantages of Taiwan. For example, Firewall/UTM products are based on the advantage of integrating network communication hardware. E-mail security is based on the advantage of two-byte languages. PKI/Crypto encryption/decryption products are based on the advantage of academic R&D solutions.
- The industry can develop competitive technologies and value-added products by leveraging the distinctive characters that Taiwan has, the technology and market trends, and the specific attack-types received from China.

Note 1: This figure covers 41 local Taiwanese ICT security product vendors. It excludes foreign companies and ICT security distributors/service providers.
Note 2: The "日(J)" indicates products exported to Japan.
Source: III MIC (June 2009).

Taiwan Industry's Difficulties in the Current Market

- **Domestic Market**
  - ICT security market in Taiwan is limited and fully opened. Local vendors have to compete with multi-national companies having well-known brands.
  - Domestic vendors are usually small without enough marketing resources. On the other hand, smaller corporations have limited ICT security budget. Enterprises/larger corporations are the major customers in Taiwan's ICT security market.
  - Enterprises are concerned with the reliability of the product, and favor imported brand-name products. Domestic developed products have limited chances.
- **Global Market**
  - The cost for international marketing is very high. To build a brand name is a long term process.
  - To sell security products has to provide customer service for installation, renew, etc. Vendors in Taiwan can not afford customers services in the foreign countries.
  - Without well-known brand names, companies do not have strong bargain power to negotiate with distribution channels .
  - Reliability is a key concern in security products, not price. Taiwan vendors are usually smaller without well-known brands. It is difficult for them to compete with international brands.
- **General Issues**
  - Establishing security technology takes time. Domestic vendors do not have enough resources to invest the development and foster ethical hackers.
  - Security companies in Taiwan develop products individually, but they do not collaborate to provide a total solution. It makes hard for them to compete with international companies.

Regulation Enforcement Status in Taiwan

- **Current Progress in ICT Security Related Legislation:**
  - The draft of “Amendment to the Computer Processed Data Protection Act" is being reviewed in the Legislative Yuan;
  - The Legislative Yuan requires NCC to negotiate with the relevant units and then re-submit the "Junk E-Mail Statute";
  - Neither the version of the HIPAA nor that of the Sarbanes-Oxley Act (SOX) has been drafted in Taiwan
- **ICT security classification scheme only specifies which types of ICT security defenses are required.**
  - Existing ICT security classification guidelines only require government agencies to acquire ICT security products and ensure both the breadth and depth of their defense. The guidelines do not specify the principles or standards to which the ICT security products must obey, such as their countries of origin or the certificate of the products.
  - China has setup five levels for ICT system protection. Government agencies above a certain level may only use products made by Chinese ICT security vendors .
- **International ICT security certification is very extensive and complicated. It is very difficult for domestic developers to comply due to their relatively small size.**
  - The Common Criteria (CC) that are used internationally involves various and difficult certifications. This is quite expensive and beyond the ability that domestic vendors can offer; thus, if the domestic products are required to comply, the market would be wide open to international brands .

Previous Research Achievements in Taiwan

Technology Type	Main Academic/ Research Effort	Key Technologies Mastered
Threat Management （FW,IDP/IPS,UTM..）	NTUST, NCKU, NTHU, NDU, NCU, III	- Intrusion Detection Platform (IDEAs) - Simulated Test Platform (TWISC@Testbed) - DS capability probing (IDS Probing) - URL and Web filtering (WAF)
Content Security (Botnet detect, Anti-Virus/Malware, Email Security..)	NSYSU, NCKU, NCTU, NTU, NTUST, NDU, Tatung, III	- Anomalous IRC Traffic Analysis - Malware Behavior Analysis
Vulnerability Management (VA Scan, Pen Test, SIEM/SOC, Source Code Security..)	NTU, NSYSU, Academia Sinica, NDU, III	- Source code checking - Network security assessment system (SAS) - Vulnerability scanning platform (CVS)
Mobile Security (Mobile Protection/ Privacy, Wireless Security..)	NCTU, CYCU, NCU, ICTRI	- Secure wireless overlay observation network (SWOON) - WiFi wireless penetration
Identity Authentication and Access Management (PKI, AAA)	NCKU, NTUST, CHTTL	- Electronic polling (e-Vote) - National Certification Center

Research Investment (Unit:NT$1,000)	95	96	97	98
Academia (NSC Fund)	171,101	193,186	169,557	106,521
III & ITRI (NSC&MOEA Fund)	74,333		72,529	72,480

Taiwan Industry Opportunities & Advantages

- **Emerging ICT Security Demands from Cloud Computing Services:** The special characters of cloud computing service, multi-layer technical architecture and dynamic computing infrastructure, lead to more ICT security threats and demands. Taiwan vendors can establish their niche in this area in the earlier stage. The upstream suppliers and downstream vendors can collaborate to enlarge their scale.
- **Increasing Importance of Mobile Security:** Given that the rapidly growth of security threats in mobile applications, Taiwan's solid foundations in mobile applications and products provides a great opportunity to enter this emerging market.
- **A Strong Network Communications Industry:** Taiwan have the competitive advantage in ICT hardware development and have hardware-and-software integrated products, such as firewalls/UTM. In the future, web application layer protection or other high-end protection features can be added into these products that will increase their value.
- **Leading-knowledge of Specific Attack Models:**
  - Taiwan's sensitive political-economic position provides good opportunities for learning specific ICT security attack models and this can be exploited for developing niche ICT security products.
  - Since Taiwan uses a double-byte language, this can be combined with its expertise in e-mail filtering products to develop malicious software filtering products and boost industry competitive advantages.

IV. Development Strategy and Action Plans

Industry Development Visions & Goals

Visions

1. Support the iTaiwan project to satisfy critical ICT security demands.
2. Develop innovative ICT security technologies to stimulate industry growth and to create new opportunities

Goals

1. Boost Taiwan ICT security industry to 30 billion NTD within 5 years and generate the revenue of derivative ICT security related products to 170 billion NTD*.
2. Promote at least one large-scale critical ICT security application in cloud computing services.

* Derivative ICT security related products include network equipment and terminal devices with integrated ICT security features.

Major Strategies for Facilitating the Development

- Expand and consolidate the domestic market in order to strengthen Taiwan ICT security industry and to boost market share.
- Policy support critical technologies and applications to develop application-oriented technology products that will strengthen both Taiwan ICT security standard and the industry's international competitive advantage.
- Support advanced research and expertise by investing in the next-generation ICT security industry to give the industry a head start.

Strategy 1 – Expand & Consolidate Domestic Market

- **Proposed measures**
  - **Establish an ICT security promotion project to facilitate development of the domestic industry (IDB);**
  - **Leverage Taiwan's industry advantages (e.g. industrial computers, ICT products, IC design, etc) by using policy tools and incentives to encourage vendors to develop ICT security products (IDB, DOICT);**
  - **Encourage government agencies to use domestic ICT security solutions without violating GPA regulations. It will not only gather practical experiences, but also can create success cases for the international market.(PWC, IDB);**
  - **Encourage vendors to adopt local ICT security solutions in conjunction with the iTaiwan project (MOTC, MOI, MOEA, RDEC, CCA) ;**
  - **Guide companies to acquire international certifications; and assist them to expand the international market (IDB, DOICT)**

Action Plan– Assist the Industry with ICT Security Product Development and Market Initiative

Action Items

1. Work with the Security Industry Promotion Plan to provide assistance on emerging ICT applications and establish a consultation and grant mechanism.
2. Reply to the needs of the ICT security in the iTaiwan project, introduce ICT security applications for mobile commerce and digital contents.
3. Use a software-supports-hardware and hardware-leads-software approach to assist vendors with the development of integrated hardware-software benchmark products and encourage them to enter the international market.

Expected Outcomes

- Complete at least 10 ICT security product development or value-added assistance cases.
- Develop at least 2 ICT products that integrate hardware and software products and promote one product to the international market.

Budget Requirement

Year	99	100	101	102
Budget *(Unit:NT$1000)*	96,000	96,000	96,000	96,000

Strategy 2 – Policy Support Critical Tech &Apps

- **Proposed measures**
  - **Invest resources in the development of critical ICT security technologies for cloud computing services and mobile applications as well as supporting demands from emerging applications (DOICT);**
  - **Use ICT security programs to coordinate major domestic ICT service vendors and use their critical technologies to develop a secure cloud computing service platform (DOICT, DIB, NSC);**
  - **Attract major foreign security companies to set up ICT security research/testing centers in Taiwan (DOICT);**
  - **Leverage "Smart Town" and "i-Park" application environments in the i236 project to provide a playground for local ICT security solutions (DOICT);**
  - **Apply the flagship model to encourage alliances or mergers between key vendors to enter the international market (IDB, DOICT)**

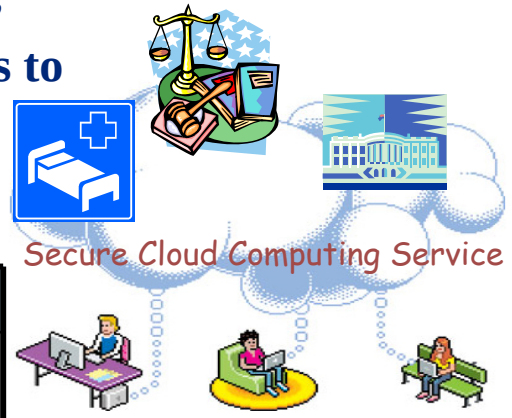
Action plan - Develop Cloud Computing ICT Security Technologies to Seize the Advantages in the Market

➢ Action Items

1. **Developing key security technologies for cloud computing services**
   - **Application Layer Protection:** Develop content filtering and protection technologies targeted at the dynamic computing infrastructure in cloud computing
   - **Secure Cloud Computing Platform:** Develop an integrated monitoring and management solution based on a secure cloud computing platform system
2. **Applying developed security technologies into large-scale applications (target on high-demanded areas)**

➢ Expected Outcomes

- **Complete at least 2 ICT security platforms requiring cloud computing services;**
- **Complete at least 1 critical large-scale ICT security application;**
- **Promote at least two homegrown ICT security products/services to the international market**



➢ Budget Plan

Year	99	100	101	102
Budget *(Unit: NT$1,000)*	151,719	152,000	160,000	160,000

Strategy 3 - Support Advanced Research & Expertise

- **Proposed Measures**
  - **Encourage academic development and operation of advanced ICT security offensive/defensive simulation platforms to strengthen the applicability of local research results and their competitive advantages (NSC);**
  - **Encourage academic development of basic ICT security verification/testing technologies and the provision of professional testing services (NSC);**
  - **Encourage academic engagement in pioneering ICT security R&D in accordance with industrial development policy and cultivate experts in ICT security technologies (NSC);**
  - **Establish TWISC industry-academic R&D alliance to strengthen cooperative research and accelerate the commercialization of R&D results (NSC);**
  - **Strengthen international cooperation/value creation/service delivery by the TWISC as well as strengthening its ability to sustain itself(NSC)**

Action Plan – Implement Advanced ICT Security R&D and Talent Development

Action Items

1. Use a virtual security networking environment to develop and maneuver intrusion detection and prevention security technologies against new attack types/malicious software;
2. Encourage academic R&D in ICT security certification/testing technologies and the development of multi-layer/real-world network traffic simulation testing technologies to ensure good quality of ICT products and secure communications;
3. Leverage academic resources to conduct advance research into ICT security technologies for cloud/mobile/ubiquitous computing and cultivate high-level expertise needed in the ICT security industry in Taiwan;
4. Establish a platform for attract international experts and cultivate world-class technical teams;
5. Establish TWISC industry-academic research alliances to commercialize academic research results and boost industry competitiveness

Budget Plan

Year	99	100	101	102
Budget *(Unit:NT$1,000)*	200,000	210,000	220,000	230,000

V. Topics for Discussion

- **Given that the sizes of Taiwan ICT security vendors are smaller in general, how do we help vendors become large enough to enter the international market?**
  - Use policy tools to assist vendors to continuously develop ICT security solutions;
  - Encourage industry alliances and development via the next-generation ICT security applications;
  - Encourage major international vendors to set up industry research/testing centers in Taiwan.
- **To boost the development of ICT security technologies and expertise, should a global virtual ICT security battlefield, based on online communities, be promoted?**
  - Leverage the existing academic research effort in Taiwan to cultivate professional expertise to meet industry needs;
  - Establish an ICT security offensive/defensive exercise platform to test and develop new ICT security technologies
- **To encourage ICT security companies to have security solutions ready in advnace, shall provide them the government's strategic ICT security plans for the next 5 years?**
  - By using the national ICT security meetings as a communication channel, the government will provide the industry with its medium to long-term ICT security posture and upgrade plans in advance.
- **To promote security level and expand the market size in Taiwan, shall security items be required in the regulations of company management for public companies?**