NECTEC
a member of NSTDA

Cyber Security a Global Challenge; What and how Thailand is doing

Pansak SIRIRUCHATAPONG
Executive Director
National Electronics and Computer Technology Center
February 19, 2009

Global IT Security Market

According to RNCOS

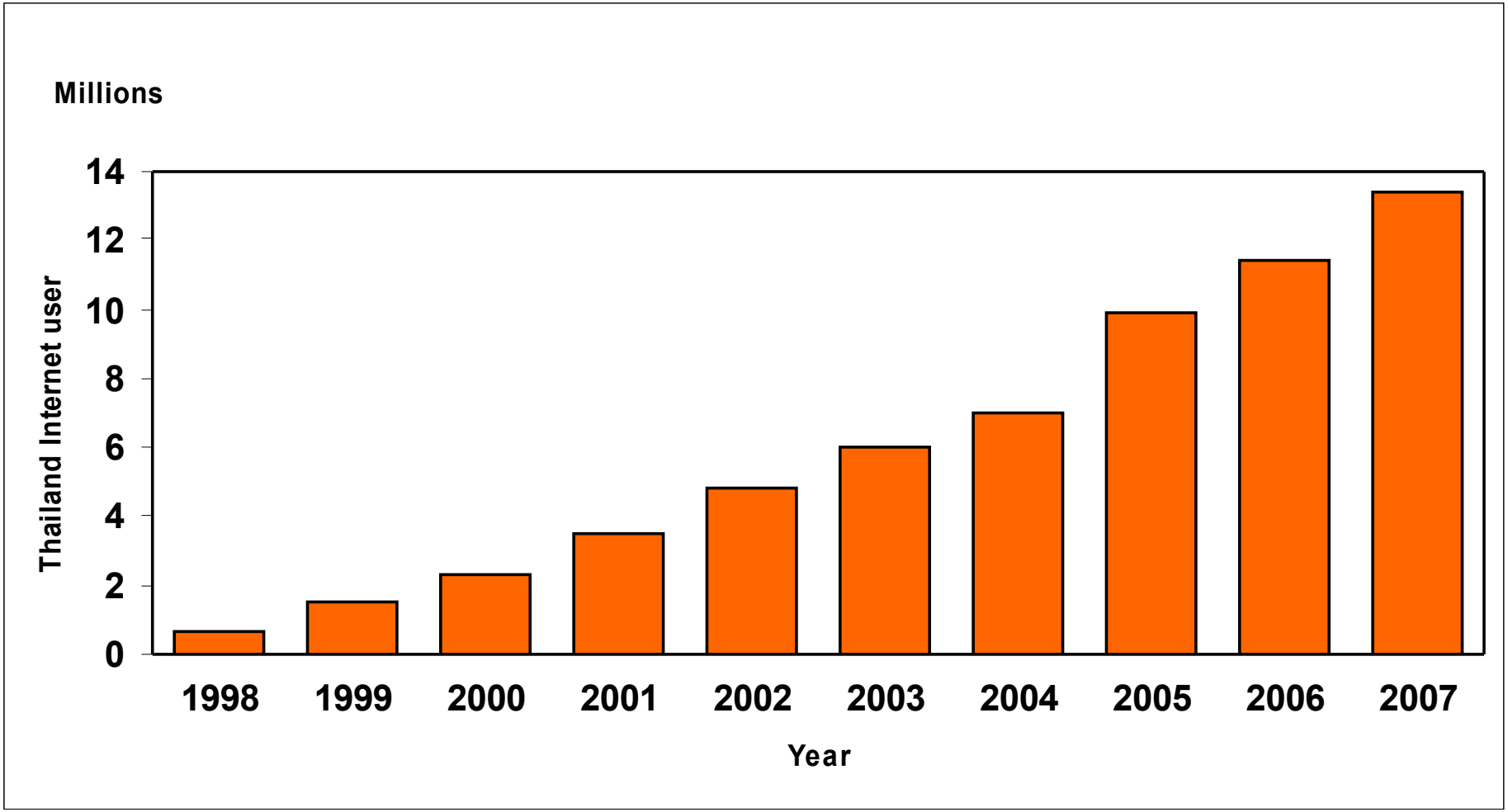
"The global IT security market (includes security software & security appliances) is expected to grow at a CAGR (Compound Annual Growth Rate) of 15.5% through 2012 from 2008, according to RNCOS

The increasing number of IT security attacks, ongoing vulnerability discoveries, and the need for companies to comply with new legislations are fostering the growth of global IT security market.

The Asia-Pacific region is anticipated to account for the majority of IT security solutions market by 2012."

Internet Usage in Thailand

NECTEC
a member of NSTDA



Source : http://internet.nectec.or.th/webstats/internetuser.iir?Sec=internetuser

Thailand IT Security Market

- Thai Government 's enforcement of the **Computer Crime Act** B.E.2550 (2007) create **awareness in businesses** about **information security**. It alerts businesses to **protect their information technology system** and requires businesses to keep computer traffic data for at least 90 days. This is the driver to **push Thailand IT security market growing**.
- Overall **IT security market** is approximately **3,000 to 5,000 million baht** (100-150 million US$) and still **growing and expanding** in Thailand.
  - Approximately 2-million customers in government and private sectors
  - More than 50% not ready for the Computer Crime Act, and have no IT security system

Threats Continue to Evolve

หมายเหตุ รูปแสดง **Cyber Threat** ต่าง ๆ ที่กำลังเป็นปัญหาอยู่ในปัจจุบัน ปัญหาใหญ่ในวันนี้ก็คือ เรื่อง **Spyware, Phishing, SPAM** และ **Peer-to-Peer Exploit**

Trends Of Information Security

- Mobile Devices
- Government Action
- Attack Targets
- Attack Techniques
- Defensive Strategies
- BCP, DRP, Security Standard

Mobile Devices

1. **Laptop encryption** will be made mandatory at many government agencies and other organizations that store customer/patient data and will be preinstalled on new equipment.
2. **Theft on PDA smart phones** will grow significantly. Both the value of the devices for resale and their content will draw large numbers of thieves

Government Action

1. **Legislation :** Congress and state governments will pass more legislation governing the protection of customer information. state attorneys general and state legislatures will find ways to enact harsh penalties for organizations that lose sensitive personal information

Attack Target

1. **Government agencies :** Targeted attacks will be more prevalent, in particular on government agencies , demonstrating the failure of federal cyber security activities. Other antagonistic nations and terrorist groups will radically expand the number of attacks. Targeted attacks on commercial organizations will target military contractors and businesses with valuable customer information.

Attack Target

1. **Cell phone worms :** infect 100,000 phone, jumping form phone to phone over wireless data network. Cell Phone are more powerful. That makes them fertile territory for attackers fueled by cell-phone adware profitability
2. **Voice over IP (VoIP) :** deployed hastily without fully understanding security

Attack Techniques

1. **Spyware** will continue to be huge and growing issue.
2. **0-day vulnerabilities** will result in major outbreaks resulting in many thousands of PCs being infected worldwide.
3. **BotNet bundled with rootkits :** rootkits will change the operating system to hide the attack's presence

Defensive Strategies

1. **Network Access Control** will become common and will grow in sophistication. As defending laptops becomes increasingly difficult, large organizations will try to protect their internal networks and users by testing computers that want to connect to the internal network. Tests will grow from today's simple configuration checks and virus signature validation to deeper analysis searching for traces of malicious code

Thai's ICT laws

NECTEC
a member of NSTDA

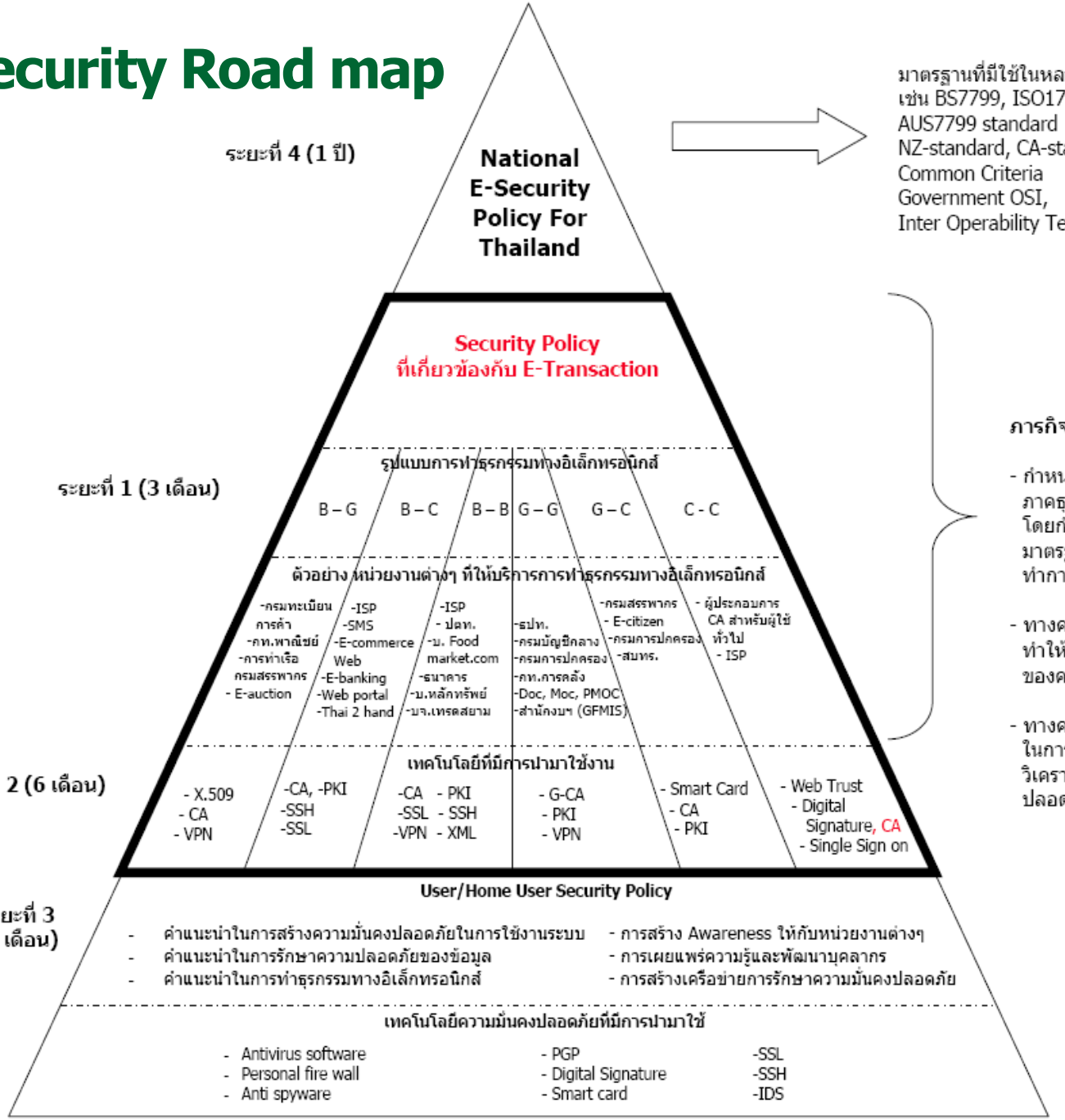
- Electronic Transaction Act 2001
- Computer Crime Law 2006
- Data Protection Law (On process)
- Electronic Fund Transfer Law (On process)

Nectec's roles in ICT Policy

NECTEC
a member of NSTDA

- Policy and Planning Development Steering Committee (คณะอนุกรรมการนโยบายและแผน)
- E-Transaction and Government Business Supervisory Steering Committee (คณะอนุกรรมการกำกับดูแลธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์และธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ)
- Legal Infrastructure Steering Committee (คณะอนุกรรมการโครงสร้างพื้นฐานทางกฎหมาย)
- E-Transaction Support Steering Committee (คณะอนุกรรมการส่งเสริมและสนับสนุนการประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์)
- Security Steering Committee (คณะอนุกรรมการด้านความมั่นคง)
- Thailand PKI Forum Steering Committee (คณะอนุกรรมการโครงการ Thailand PKI Forum)

Security Road map



มาตรฐานที่มีใช้ในหลายประเทศ
เช่น BS7799, ISO17799
AUS7799 standard
NZ-standard, CA-standard
Common Criteria
Government OSI,
Inter Operability Technical Framework

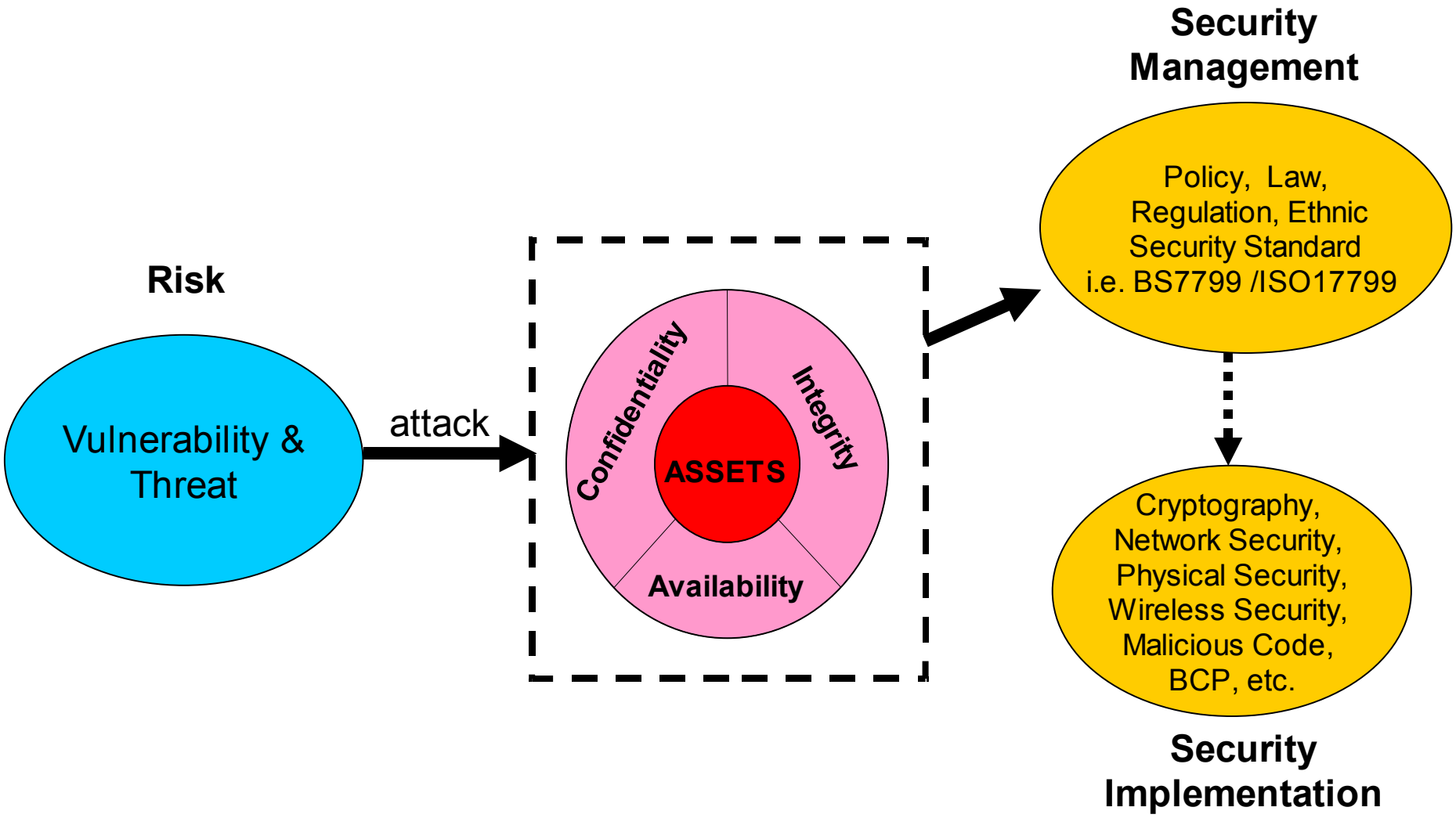
ภารกิจของคณะอนุกรรมการความมั่นคงในช่วงแรก

- กำหนดนโยบายความมั่นคงปลอดภัยให้กับภาครัฐ ภาคธุรกิจที่ให้บริการการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยกำหนดเป็นข้อกำหนดพื้นฐานโดยอ้างอิงจากมาตรฐาน ISO 17799 ที่ทางฝ่ายเลขานุการกำลังทำการศึกษาอยู่
- ทางคณะอนุกรรมการความมั่นคงหากลไกที่จะทำให้ข้อกำหนดพื้นฐานที่ผ่านการวิเคราะห์ของคณะอนุกรรมการฯได้รับการนำไปประกาศใช้
- ทางคณะอนุกรรมการความมั่นคงกำหนดลำดับก่อนหลังในการธุรกรรมทางอิเล็กทรอนิกส์ที่จะดำเนินการ ศึกษาวิเคราะห์ เพื่อกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยในแต่ละการทำธุรกรรม

<u>Roadmap</u> <u>แสดงการดำเนินงานของคณะอนุกรรมการความมั่นคงฯ</u>

<u>หมายเหตุ</u> การกำหนดมาตรฐานควรกำหนดเป็นมาตรฐานขั้นต่ำและทำการปรับปรุงทุกปี

Information Security Big Picture



How to operate Information Security

T ⟶ **T**echnology

P ⟶ **P**rocess

P ⟶ **P**eople

Causes of Security Problem

- **Technology**
  - Lack of security feature
  - Bug, hole, no patch
  - No standard
  - Hard to up-to-date
- **Process**
  - Design for security
  - Role + Responsibility
  - Audit, track
  - Disaster plans
  - Stay up-to-date
- **People**
  - Lack of knowledge
  - Lack of commitment
  - Lack of good communication
  - Human error

Nectec provide ISO/IEC 27001 (Thai's version 1.0 , 2.0)

NECTEC
a member of NSTDA

CERT ➡ Computer Emergency Response Team

An organization or a team that provides, to defined constituency, services and support for both preventing and responding the computer security incidents.

International Forum Collaboration

NECTEC
a member of NSTDA

- ThaiCERT is a full member of APCERT (Asia Pacific Computer Emergency Response Team)
  - Training collaboration on computer security techniques with APCERT
  - Incidence response coordination (continuously)
  - Incidence response drill (July 28th, 2006)
- ThaiCERT is a national CERT in Thailand supported by FIRST (Forum of Incident Response and Security Team)
- Point of contact for ITU Forum for spam mail protection

International Forum Collaboration

NECTEC
a member of NSTDA

- Play roles in APT Forum (Asia Pacific Telecommunity Forum) in raising the level of many important security issues, such as security standards, spam problems
- Play roles in e-Security Task Group under APEC TEL Working Group
- Play roles in RAISS Forum (Regional Asia Information Security Standards) in security standard activities

About ThaiCERT

NECTEC
a member of NSTDA

- Ministry of Science and Technology
  - National Science and Development Agency (NSTDA)
    - National Electronics and Computer Technology Center (NECTEC)
      - Thai Computer Emergency Response Team (ThaiCERT)
- Thailand National CERT
- Full member of FIRST, APCERT

Objectives of ThaiCERT

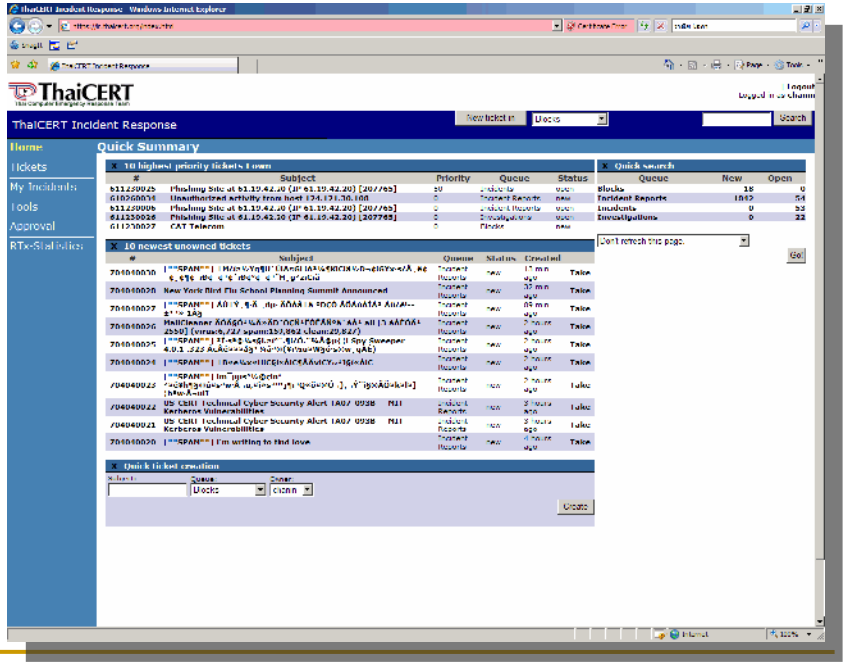
NECTEC
a member of NSTDA

- To handle the computer crime and coordinate with the related organization.
- To gain the knowledge and skill in the information security which is the factor effect to the stability of Thailand.
- To establish the team, which can handle the incidence of computer security and develop team personnel's skill.

ThaiCERT Services

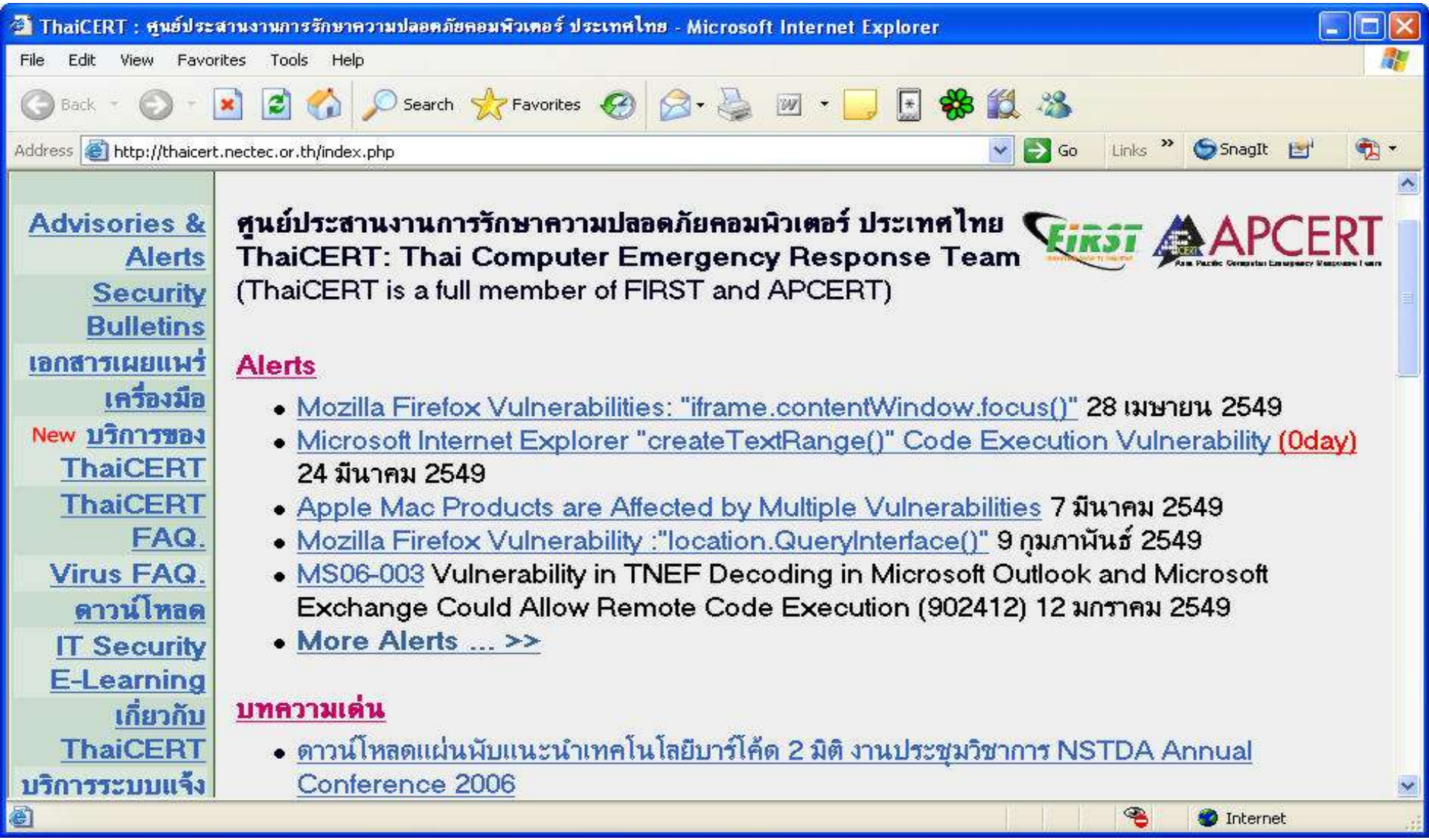
NECTEC
a member of NSTDA

- Public Services
  - User security awareness raising
    - i.e. publication of security knowledge on the web, and Safety-Net Booklet
    - E-learning on computer security
  - Incident Response
    - Virus Alert
    - Security Advisory
  - Incident Coordinator

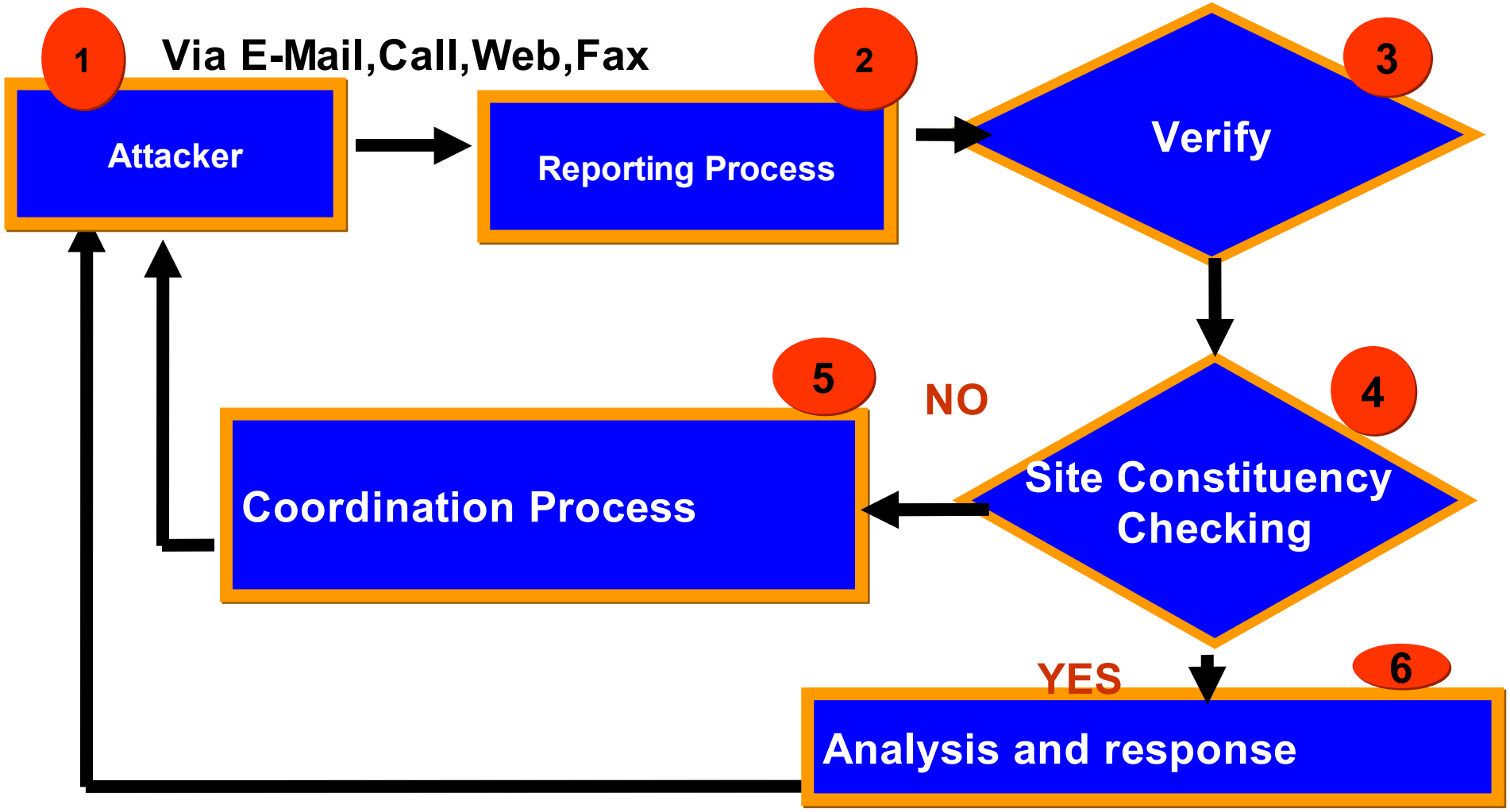


ThaiCERT Website

NECTEC
a member of NSTDA



Incident Response Process



Constituency

NECTEC
a member of NSTDA

- NSTDA and under
  - NECTEC
  - BIOTEC
  - MTEC
  - NANOTEC
- Government organizations
- some ISPs
- other organizations by request

Thank you for your attention.