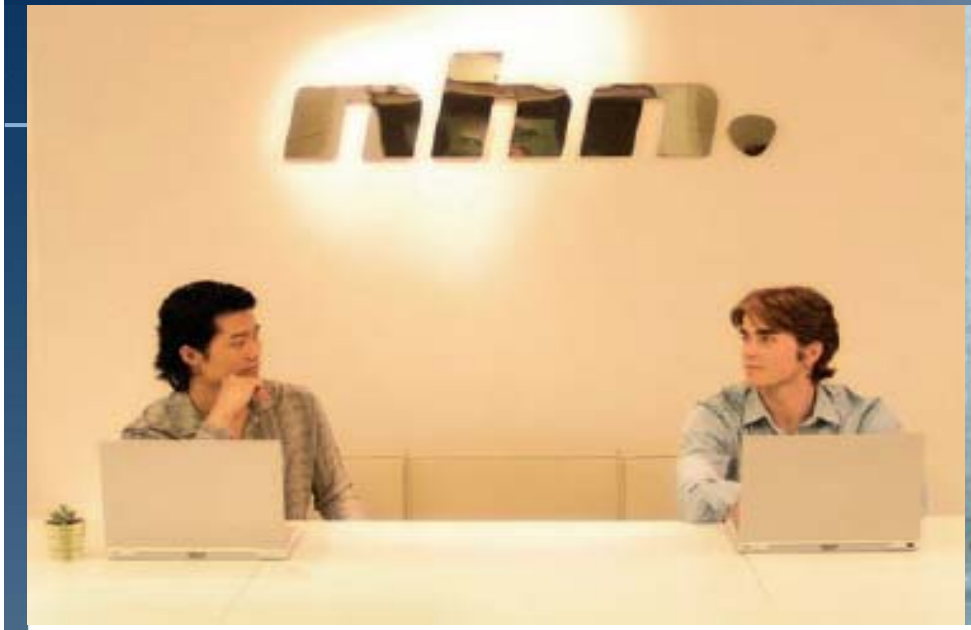


Why Security Problems are still on?

젊은 생각이 만드는 세상 - nhn.

NHN은 젊은 생각으로
새로운 네트워크 세상을 만들어
인류의 삶을 풍요롭게 합니다.

NAVER
Hangame
쥬니어네이버
해피빈

Chaeho Lim, Security Division, Ph.D

chlim@nhncorp.com

Contents

- Introduction
- Lack of Security Culture and Policy
- Lack of Security Basic Understanding
- Lack of against New Type Attacks
- Lack of Cooperation and Leading
- To Be Done
- NHN ?

Introduction

- What is Cyberspace's Security Problems?
- Why Security Issues are Still On?
- What's the Problems of the Current Security?
- What Can We Do?

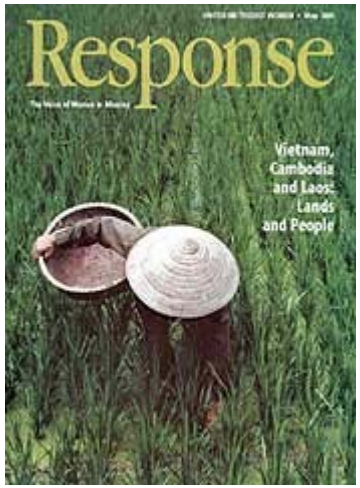
Introduction

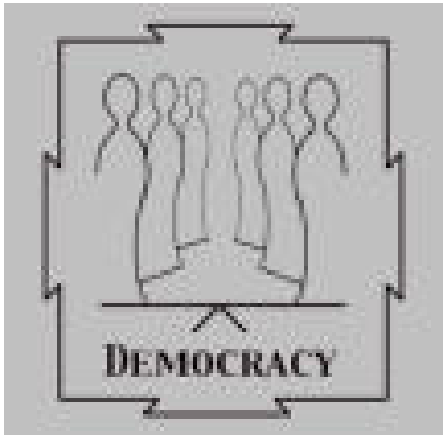
- Chaeho Lim, Ph.D.
  - He worked to set up “Korea Research Environment Open Network, KREONet” which is the first R&D network and had the first international Internet leased line from 1989.
  - Also he started to organize the working group of hacking and Anti-Hacking, Korea Internet Security Group, in Korea first.
  - As a member of KISA, the first org of security by government, he operated krCERT from 1996, and joined FIRST.ORG at first from Asia countries in 1997.
  - He tried to promote Internet security administration toward government, R&D, banking and other sectors in Korea.
  - Before a member of NHN.COM, he tried operate security venture company, SecurityMap.com but it’s failed.
  - And he worked as visiting professor of KAIST.

Lack of Security Culture and Policy 1

Cyber and Internet

What is right ?





Lack of Security Culture and Policy 2

- OECD Security Guideline
  - Awareness
  - Responsibility
  - Response
  - Ethics
  - Democracy
  - Risk Assessment
  - Safeguard
  - Security Management
  - Reassessment

Korea, What Items Were Focused ?

1. **Safeguard, FW/IDS/Anti-Virus**
2. **Response, CERT**
3. **Risk Assessment, Penetration Test**
4. **……**

Lack of Security Culture and Policy 3

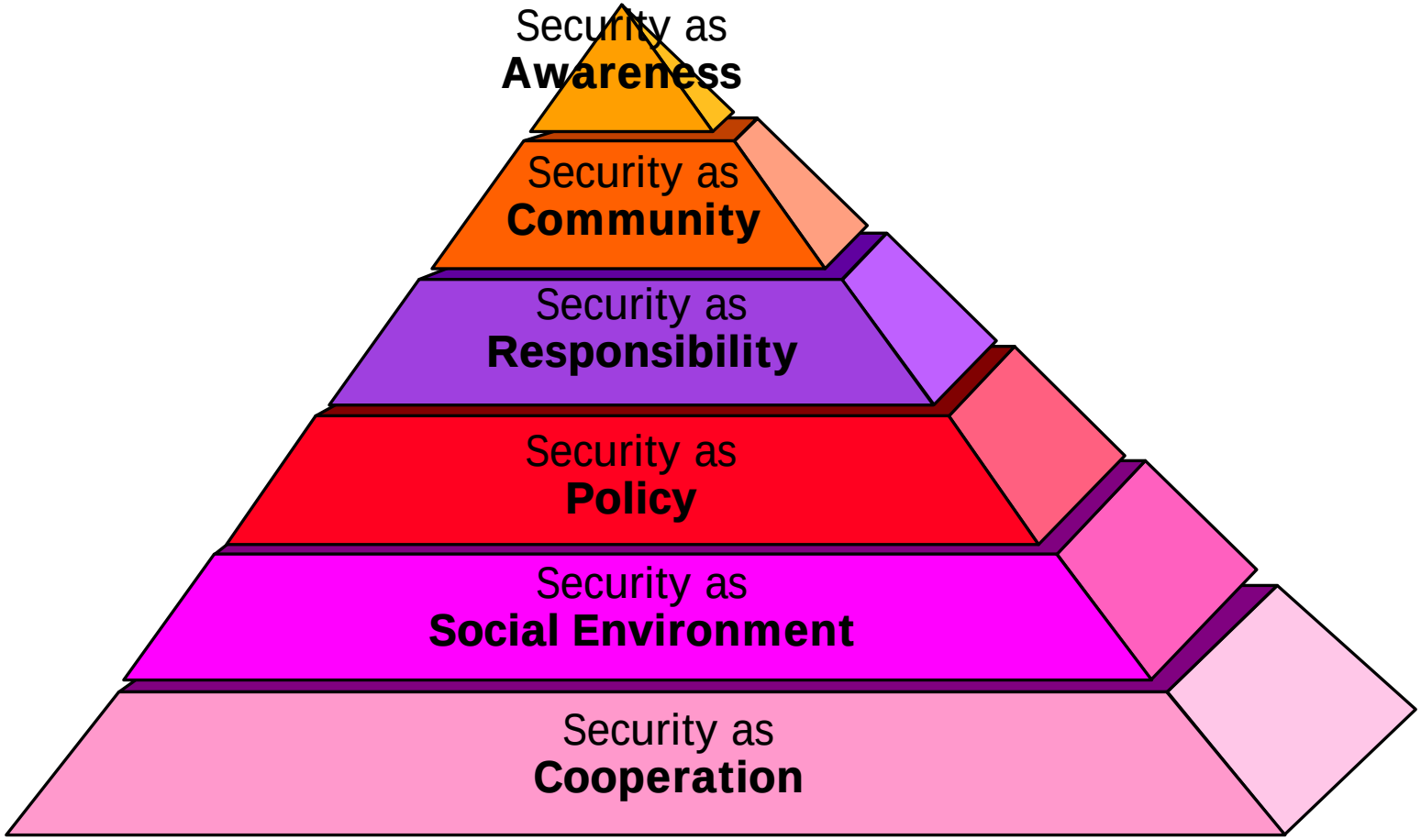
- Each participant in information systems and networks is an important actor for ensuring security.
- Participants should be aware of the relevant security risks and preventive measures, assume responsibility and take steps appropriate to their roles and positions to enhance the security of information systems and networks.”

(OECD Guidelines, 2002)

- In Korea, I launched “Consortium of CERT, CONCERT” in 1996 from Korea Information Security Agency in order to promote the security cooperation.

Lack of Security Culture and Policy 4

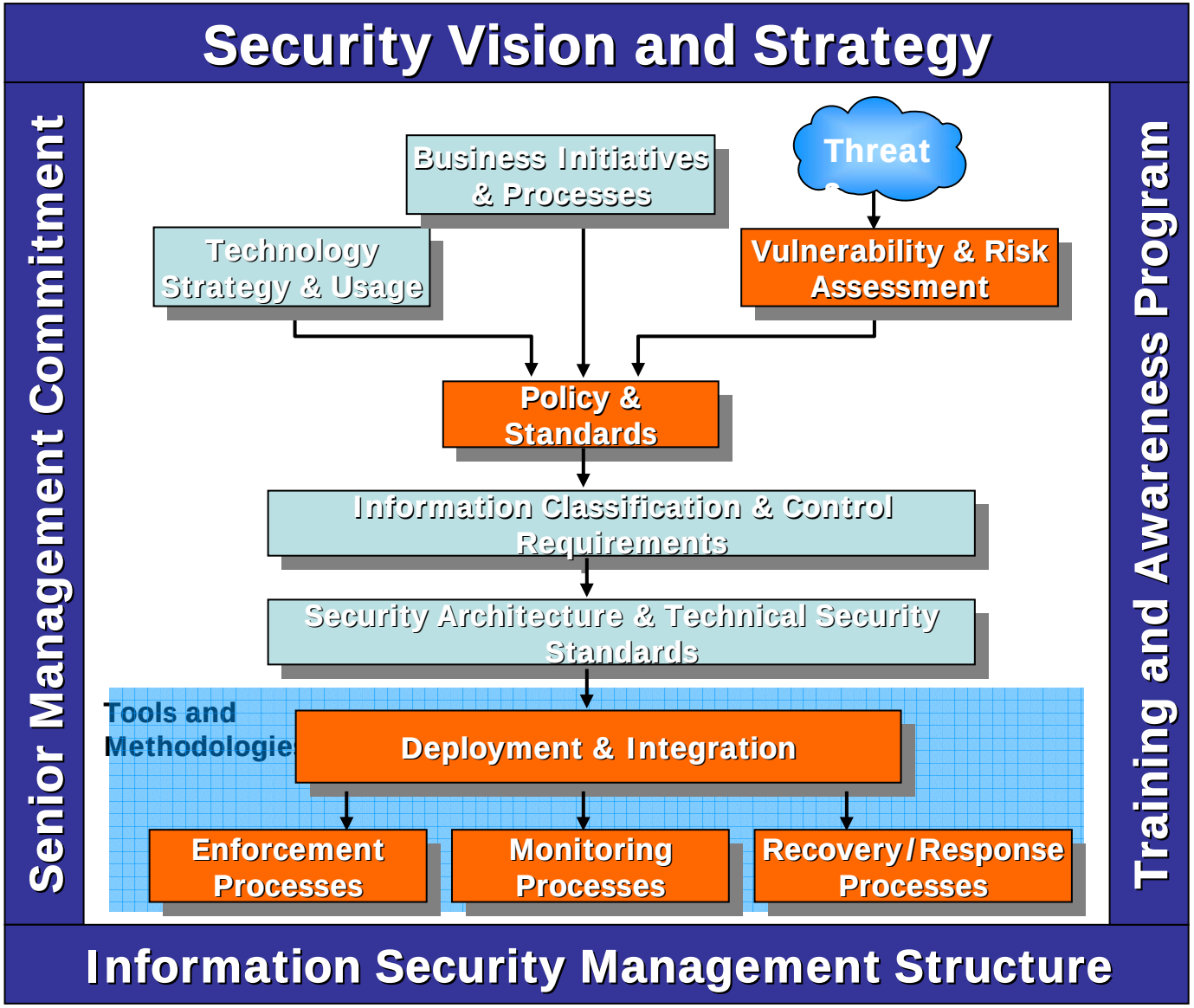
- Security Role and Responsibility



Lack of Security Culture and Policy 5

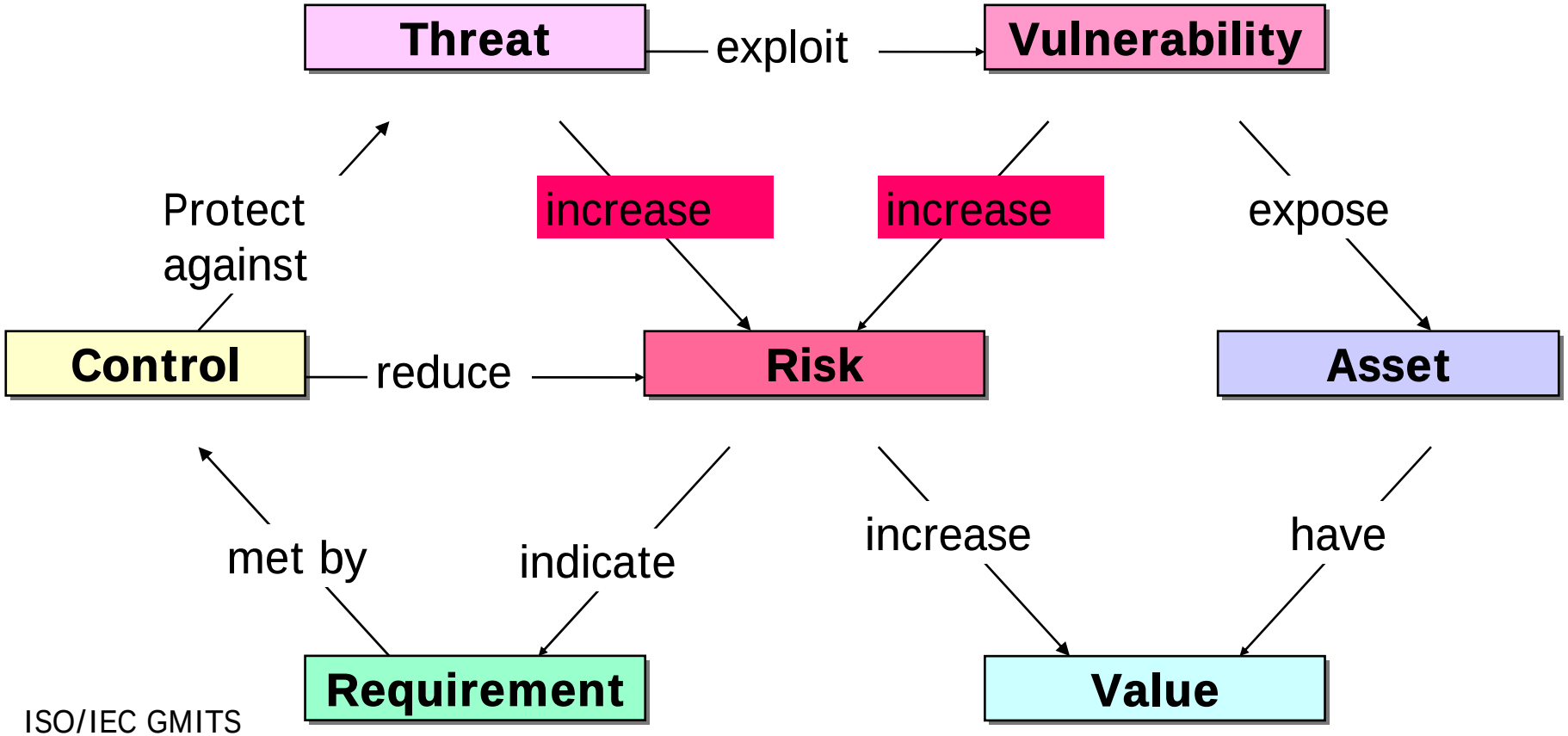
- Korea failed security because of lack of Security awareness promotion
  - You know 125 Impact by Slammer worm?
  - Korea Internet was disabled for a week
  - All didn't understand the Importance of Security Awareness
- Security Awareness
  - Understand, Knowledge, Action
  - We should make policy, guideline, law
  - And we need proper and natural security culture
  - I hope all people should not talk " I didn't know that".

Lack of Security Culture and Policy 6



Lack of Security Basic Understanding 1

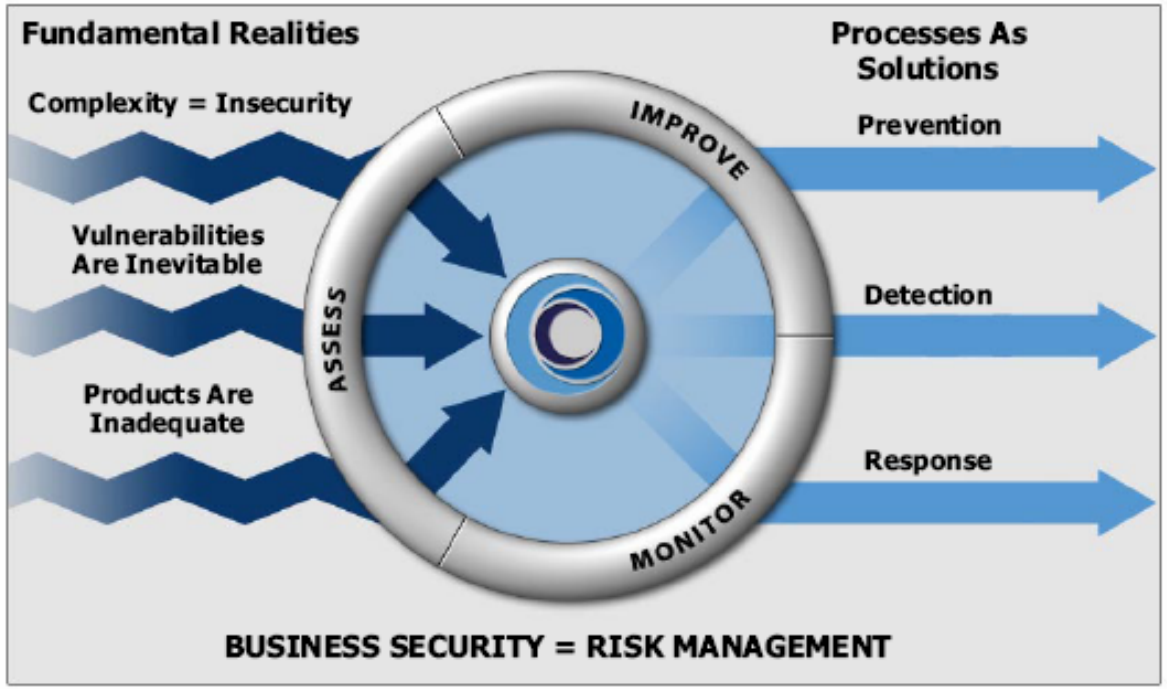
- What is Security Management?
  - Risk Management 필요, 지금까지는 Control 만 하였음



ISO/IEC GMITS

Lack of Security Basic Understanding 2

- **Complexity, Vulnerability, Inadequate Products**
- **→ Process : Protection / Detection / Response**



www.counterpane.com

Lack of Security Basic Understanding 3

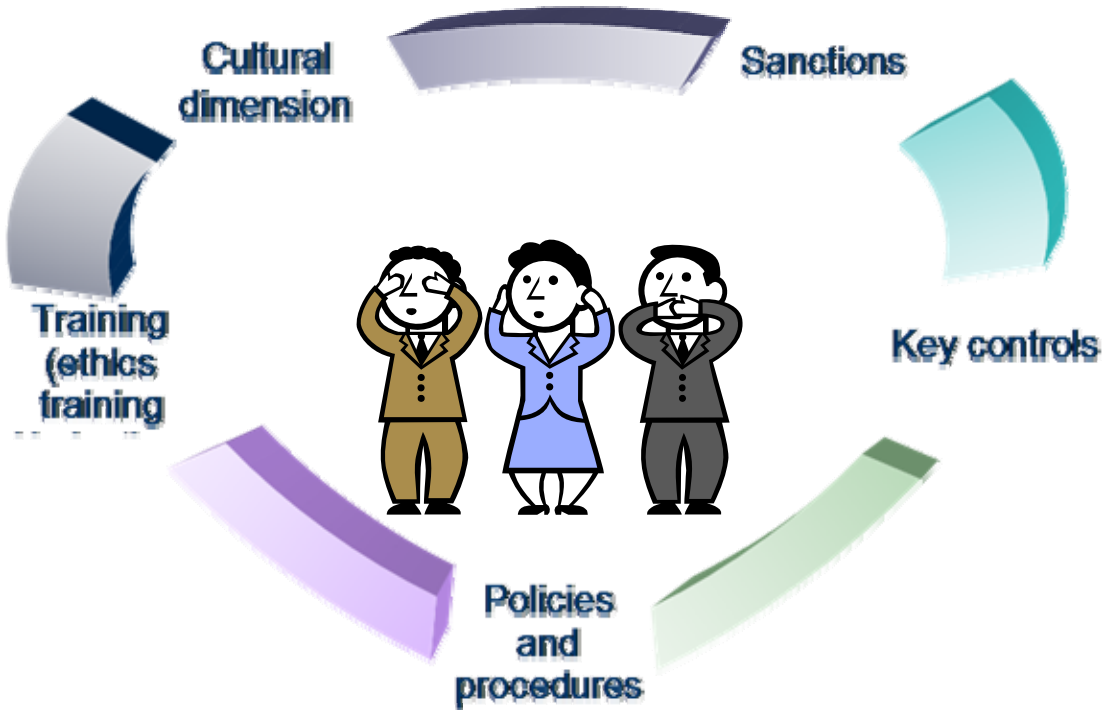
Security Management and Processes Background

Security Processes

- **Information Risk Management Process**
  - Information Security Training and Awareness
  - Risk Assessment
  - Policy Management
  - Security Architecture
- **Information Threat Management Process**
  - Threat Assessment
  - Threat Monitoring
  - Change Control
  - Incident Response
  - Incident Investigation And Forensics
  - Virus Management
- **Information Asset Management Process**
  - Account Management
  - Resource
  - Resource Management
  - Asset Classification
- **Information Vulnerability Management Process**
  - Vulnerability Assessment
  - Vulnerability Monitoring

Lack of Security Basic Understanding 4

Integrity



- Policy and Procedure
- Key Control
- Sanction
- Training
- Cultural Dimension

Lack of against New Type Attacks 1

- Denial of Information, DOI Attacks under Web2.0 Environment
- Malicious Code Attacks from China
- Privacy Attacks

Denial of Information, DOI Attacks under Web2.0 Environment [1]

Tim O'Reilly

1. **The Web As Platform**
2. **Harnessing Collective Intelligence**
3. **Data is the Next Intel Inside**
4. **End of the Software Release Cycle**
5. **Lightweight Programming Models**
6. **Software Above the Level of a Single Device**
7. **Rich User Experiences**

Google™ NAVER

Denial of Information, DOI Attacks under Web2.0 Environment 2

개인 웹사이트
personal websites

도메인 이름 선점
Domain name speculation

출판
Publishing

컨텐츠 관리 시스템
Content management systems

디렉토리
Directories (taxonomy)

블로그
blogging

검색 엔진 최적화
Search engine optimization

참여
Participation

위키
Wikis

태깅
Tagging ("folksonomy")

변화의 기반 기술 AJAX, Open API, Open Source, Mash Up

서비스 신개념 대두 Web 2.0 (Semantic Web)

Denial of Information, DOI Attacks under Web2.0 Environment 3

- DOI Attacks
  - “악의적 공격자가 유용한 정보를 가장하거나, 악의적 정보를 포함시켜 유용한 정보에 대한 거부감을 일으키게 함, 결국 정보에 대한 불신감 조장”
  - 네트워크 서비스가 IM 공격의 매개체임, 즉 P2P, Instant Message, Email 등이 주된 매개체임
  - 영향
    - 네트워크 서비스가용성 제한
    - 정보의 신뢰성 수준 상실
    - 금전적 피해가능
  - Concepts
    - QoS, DOS
    - DOI ; QoI (Quality of Information) 즉 유용한 정보의 유통을 방해하는 공격, DoS개념을 포함한 자원의 소진하는 악의적 공격 포함
      - Time,
      - Cognitive processing
      - Perceptual Capabilities
      - Memories

Denial of Information, DOI Attacks under Web2.0 Environment 4

- Attacks
  - Social Engineering
  - Spam
  - Phishing
  - Pharming
  - Click Abuse and Fraud

Denial of Information, DOI Attacks under Web2.0 Environment 4

- Safeguards
  - Filtering
  - Resource-consumption
  - Meta-Information
  - Trusted Computing
  - Database keys/indices
  - Source-evaluation
  - Structuring data
  - Restricted connectivity
  - Translating data
  - Human-computer interface
  - Data protection
  - Locating data
  - OODA 모델 이용
    - 관찰(Observe), 상황판단(Orient), 결심(Decide), 행동(Act)

Malicious Code Attacks from China

- JakUpBang ; work room
  - To gain Online Game “Items”
  - Group members fight a Single “victim”
- Malicious Codes
  - Some technicians make new malicious codes
  - Not detected by antivirus and antispyware tools
  - To gain id/pswd, other privacy information

- All attacks from China
  - To gain money
  - To get secrete information
  - And Others

What we do

- Security Strategy based
  - Our own security culture and well awareness
  - Security joined by All corporate member
  - SEA ; Secure, Efficient, Assurance
  - Security Management Process by best engineers

Secure
Efficient
Assurance