Information Security 101

Dr. CHAN, King-chung Kenny

Certified Information System Security Professional (CISSP)

認可資訊系統保安專業人員

(ISC)² SECURITY TRANSCENDS TECHNOLOGY

What is Information System?

- Information system
  - Store information
  - Process information
  - Retrieve information

  - Paper-based vs. Non-paper-based

Electronic Transactions Ordinance (Cap. 553)

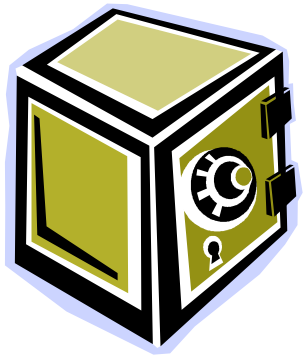
- Accord electronic record and electronic signature the same legal status as that of their paper-based counterparts

- Establish a voluntary recognition scheme for certification authorities to enhance public confidence in electronic transactions

What is Information Security?

Preservation of

1. Confidentiality,
2. Integrity, and
3. Availability of information



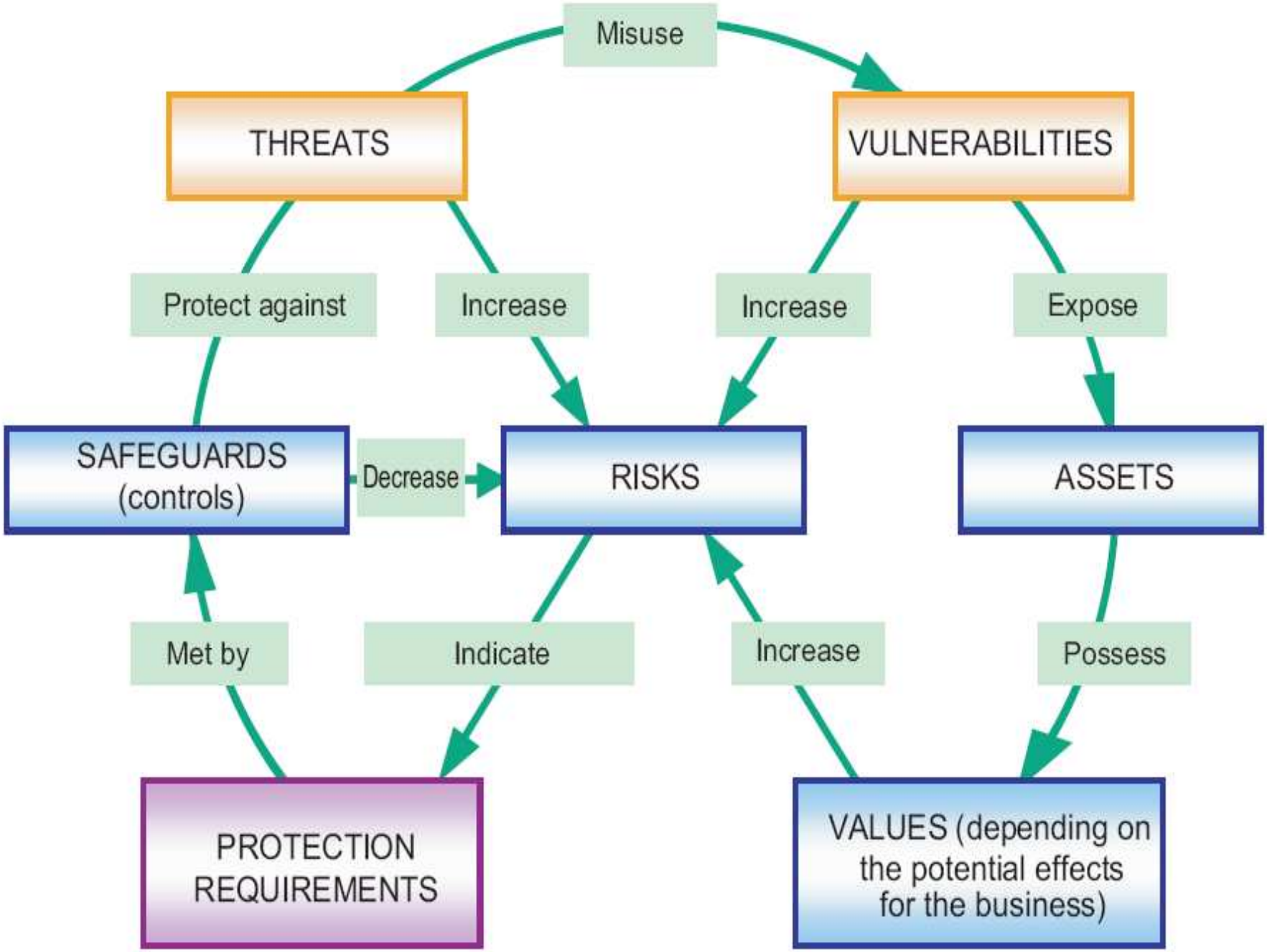
ISO/IEC 17799:2005

Information Security in CIS

- Legal requirement for security in US
  - Health Information Privacy & Portability Act
- Part of physiology monitor (medical device)
  - Stringent control by FDA in US
  - Quality assurance by ISO 13485 in EU and other parts of the world

Some Aspects of Information Security

- Access Control
- Business Continuity & Disaster Recovery Planning
- Legal, Regulations, Compliance, & Investigations
- Operations Security
- Physical Security
- Risk Management
- Network Security


Misuse
THREATS
VULNERABILITIES
Protect against
Increase
Increase
Expose
SAFEGUARDS (controls)
Decrease
RISKS
ASSETS
Met by
Indicate
Increase
Possess
PROTECTION REQUIREMENTS
VALUES (depending on the potential effects for the business)

Risk Management

- Risk Assessment
  - Probability
  - Impact
  - Level of acceptable risk
- Control measures
  - Planning
  - Implementation
  - Audit

Security Controls

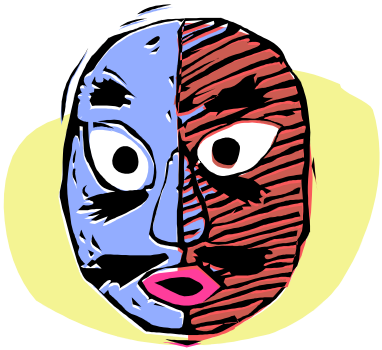
- Administrative Control
- Preventive Control
- Detective Control
- Deterrent Control
- Compensating Control
- Corrective Control

Threats - Masquerade

- Insiders
  - Using others account
  - Usually for convenience
- Service providers
  - May have legitimate reason for access
  - Unauthorized access during testing/repair
  - Secure by outsourcing arrangements
  - Rarer than insider masquerade

Threats - Masquerade

- Outsiders (Hackers)
  - Failure of
    1. User authentication
    2. Origin authentication
    3. User authorization



  - Social Engineering

Authentication vs. Authorization

- Authentication
  - You are who you claim
    1. What you have? (Staff card, e-Cert)
    2. What you know? (Passphrases, Challenge response)
    3. What you are? (Finger print, Iris scan)

- Authorization
  - Determine what you can do
- Segregation of duty

Threats – Unauthorized Use

- Application software
  - Wide range
    - Unauthorized browsing by peeping
    - Alteration of medical record maliciously
    - Identity theft
  - Failure of
    1. User training
    2. Accountability and audit control
    3. Authorization control

Threats – Unauthorized Use

- Misuse of Resources
  - Using system for personal / non-work related matters
  - Reduced availability
    - Degraded network bandwidth
    - Increased cost
  - User education
  - Mutually accepted use agreement

Threats – Repudiation

- Origin
  - Denying that they wrote something
- Receipt
  - Denying that they received a message
- Essential feature
  - Investigations into medical malpractice

Threats – Thefts

- Equipment
- Data
  - Stored
  - During communication
- Insider
  - Data of celebrity / government official
- Outsider
  - Equipment together with data it contains
- Prevention
  - Control of hardcopy output, media
  - Physical security and checks
  - Network controls

Threats – Malicious Software

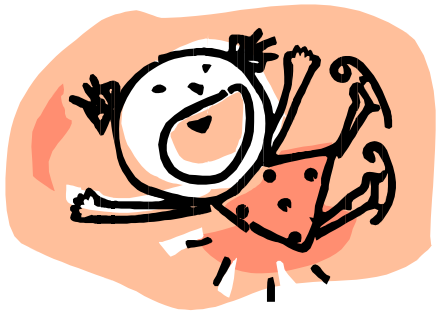
- Damaging or disruptive software
  - Viruses, Worms, Malware
  - Anti-virus protection
  - Limitation on internet / thumb drive access
- Embedding of malicious code
  - Change control
  - Audit

Threats – System Failure

- Technical Failure
  - Server
  - Software
  - Network equipment
- Environmental Support Failure
  - Power failures
  - Natural or man-made disasters
- Staff Shortage
  - Unavailability of key personnel
- Contingency Planning
- Recovery Planning

Threats – Human Error

- User Error
  - Unintentional disclosure
- Maintenance Error
  - Mis-configuration



Threats – Sabotage

- Insiders
  - Rare
- Outsiders
  - Depends on physical security control
- Terrorism
  - Theoretically possible
  - No such large-scale attacks have occurred yet

More Information

- http://www.infosec.gov.hk
  - Security Policy
  - Security Guidelines
  - Risk Assessment & Audit Checklist
  - Incident Handling Guidelines
- http://ha.home/infosec/
  - HA's Internal Guidelines