Joint Universities Computer Centre Limited
(“JUCC”)
Information Security Awareness Training- Session One

Data Handling in University

Human Factor in Information Security

Agenda

- The Information Security Concept
- The CIA Triad
- Managing Information Security
- Information Security Controls
- Human Factors in Information Security
- Information Security Roles and Responsibilities
- Improving Information Security – Human Factors

Human (procedural) versus Technical (automated) IS controls:

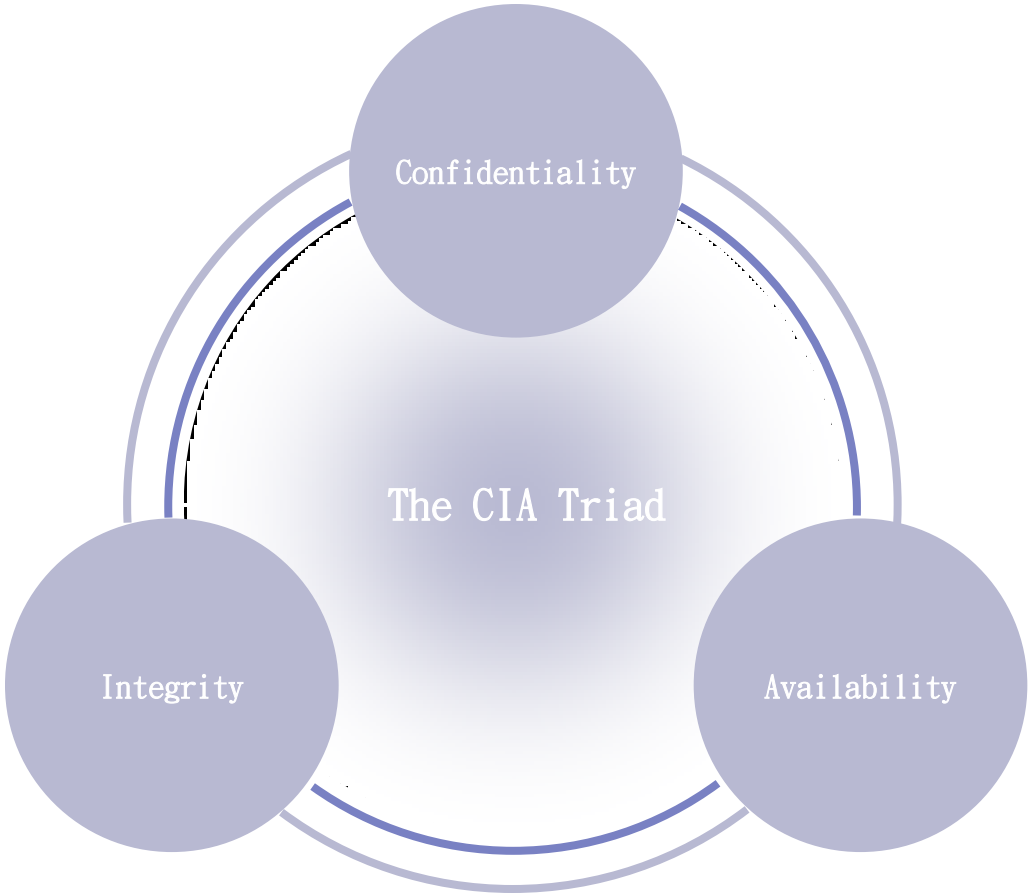
"Information security is both a human and a technological problem."
(Gary Hinson, IsecT Ltd)

Examples:

With an organisation-wide IS policy and standard in place, do users understand the need to choose strong passwords, keep them secret, and change them often? Does a system administrator check that users follow the guidance? Are the new releases of software programs checked before implementation to the production network? Does the programmer knows whether or not a new release is suitable?

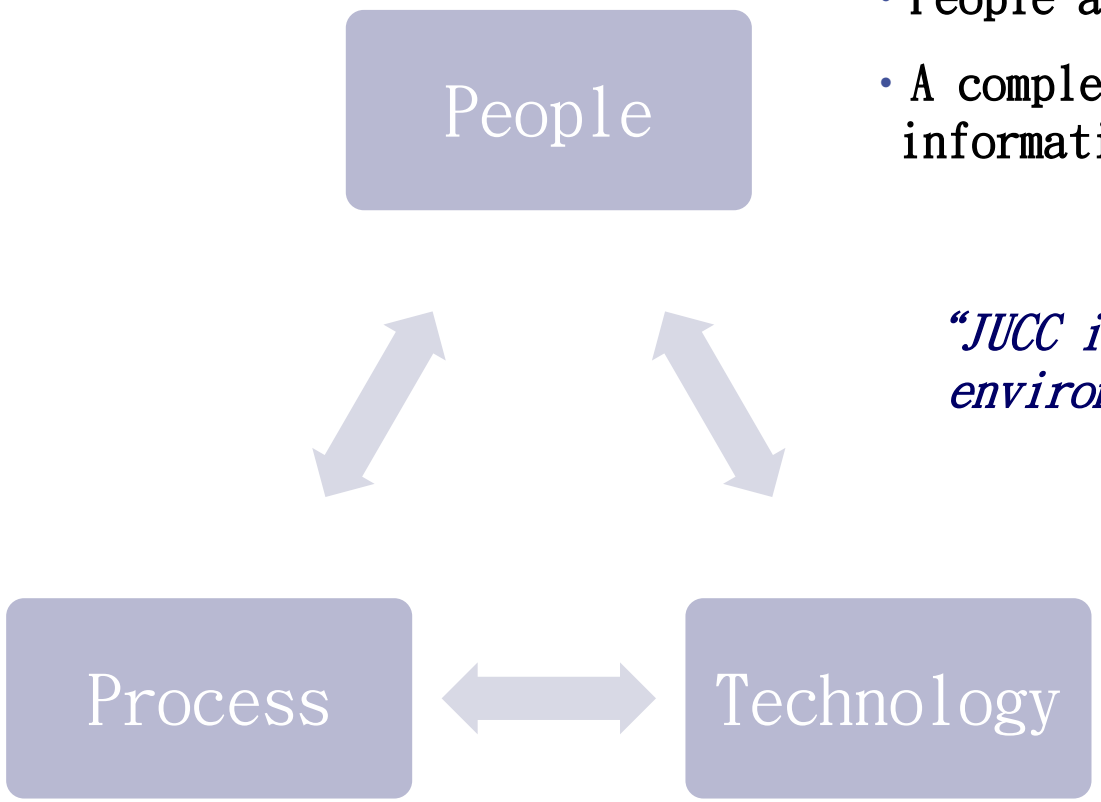
The core principles of information security:

- “Confidentiality” is keeping sensitive information protected
- “Integrity” is keeping information intact and valid
- “Availability” is keeping information available and accessible



Managing Information Security

- Information security is not only related to computer systems.
- People are always the weakest link.
- A complete framework is required to manage information security.

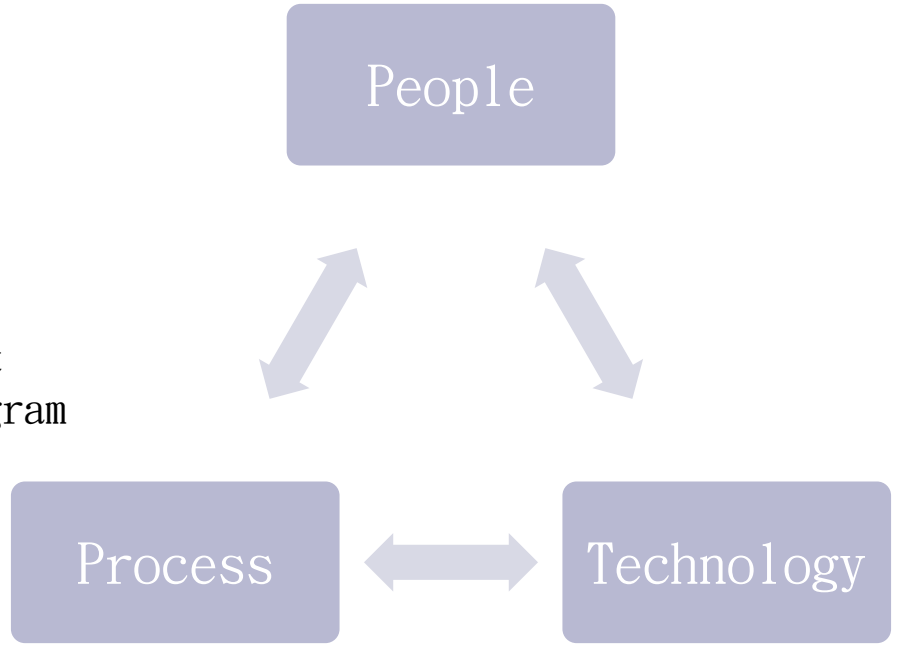


"JUCC is committed to improve the security environment of the universities in all 3 perspectives"

Managing Information Security

Process

- Regular monitoring
- Security hardening
- Effective incident management
- Patching management
- User awareness program
- Information classification
- IT risk assessment
- Internal audit
- Penetration testing
- Change management
- Security news update



People

- Management commitment
- Technical capability
- Security awareness
- Corporate culture
- Communication

Technology

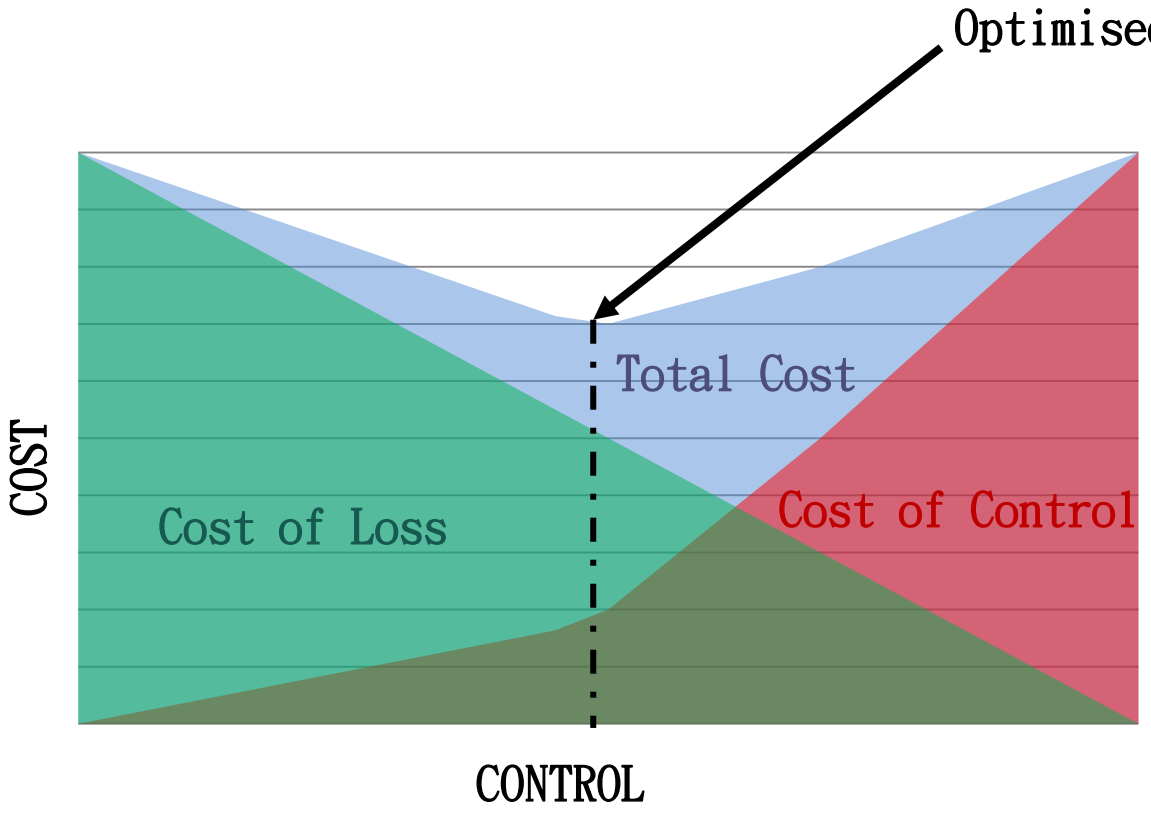
- Antivirus
- Firewall
- Intrusion Detection System
- Security patches
- Security logging

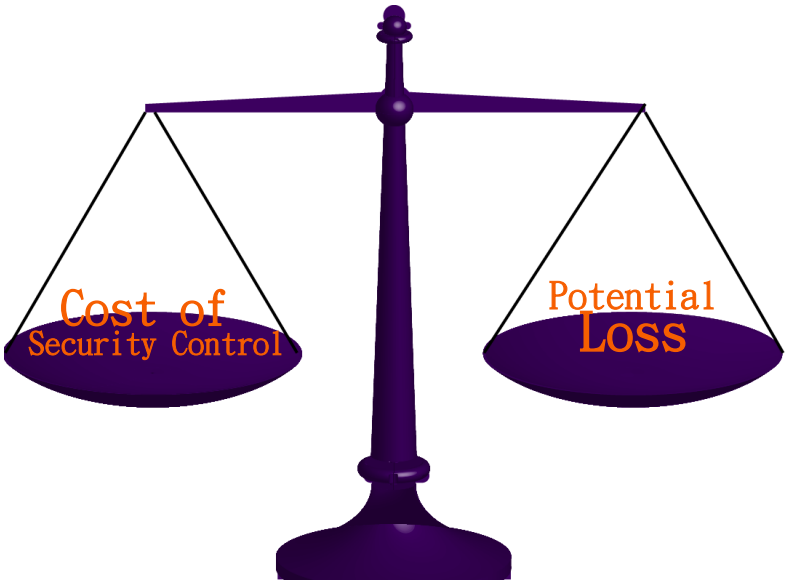
Types of Information Security Controls

Limitations

- No 100% assurance
- Breakdown e.g. misunderstand/ mistake
- Involve human judgement
- Management override
- Collusion

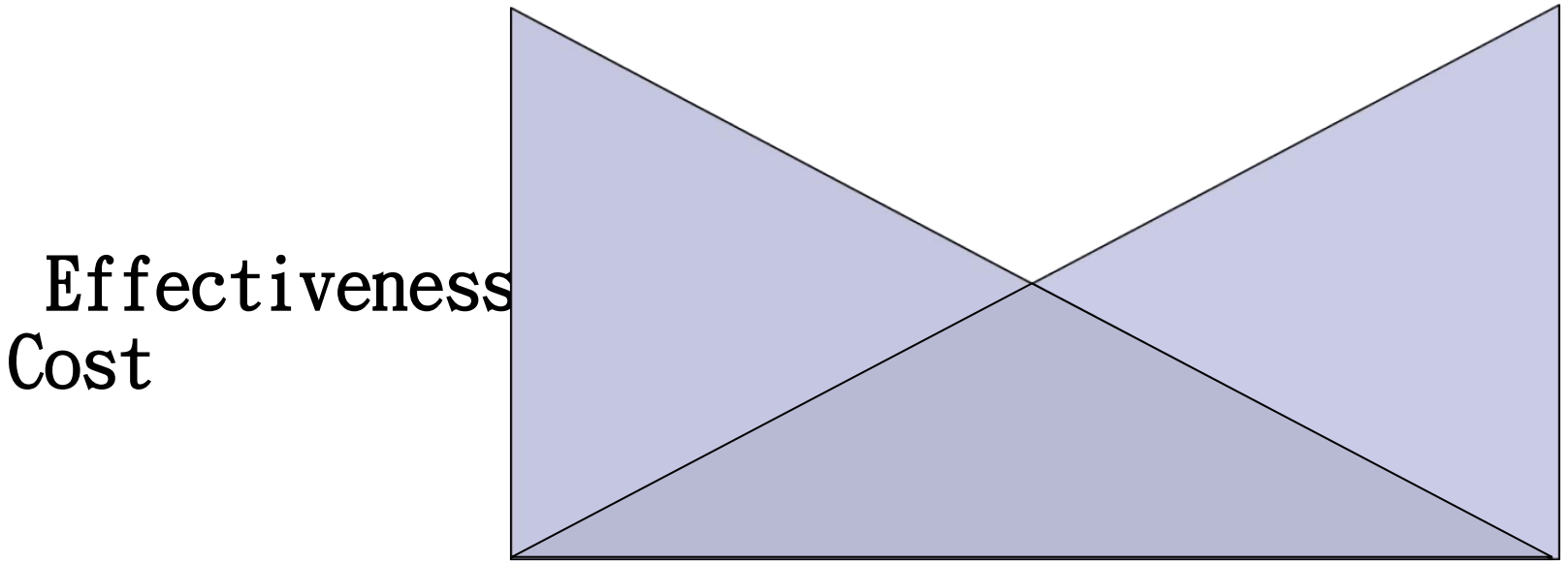
Control Implementation- Cost vs Loss

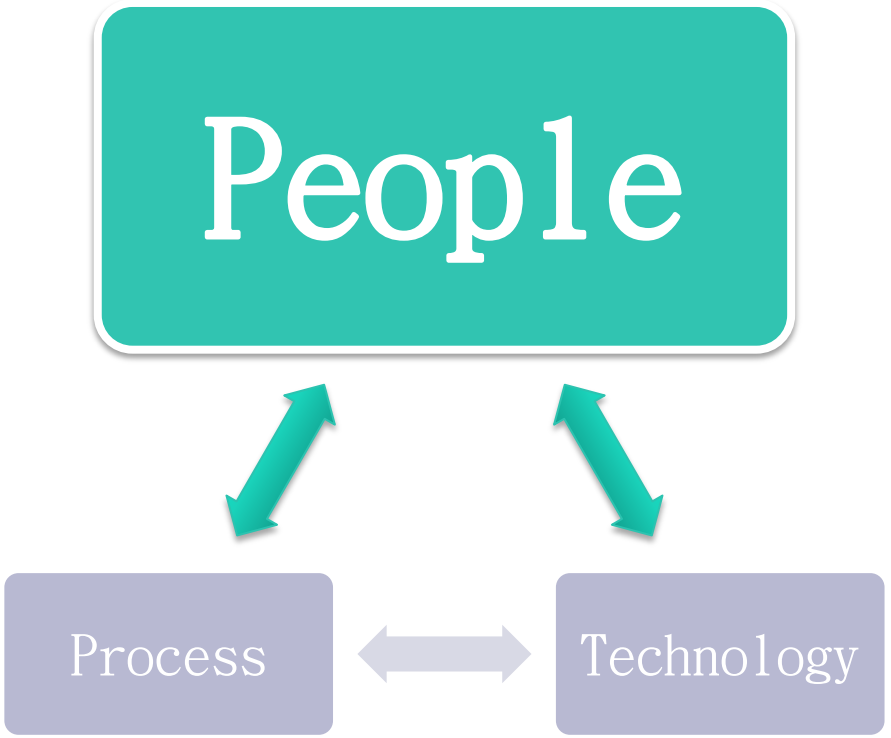




Information Security Controls

- The Cost-Effectiveness of Information Security Controls shows that "*An ounce of prevention is worth a pound of cure*" (Benjamin Franklin) as preventive controls reduce or eliminate the impact costs.
- However, no control is 100% effective, corrective and detective control can always be implemented together with the preventive control.





Why it is not just about Technology?

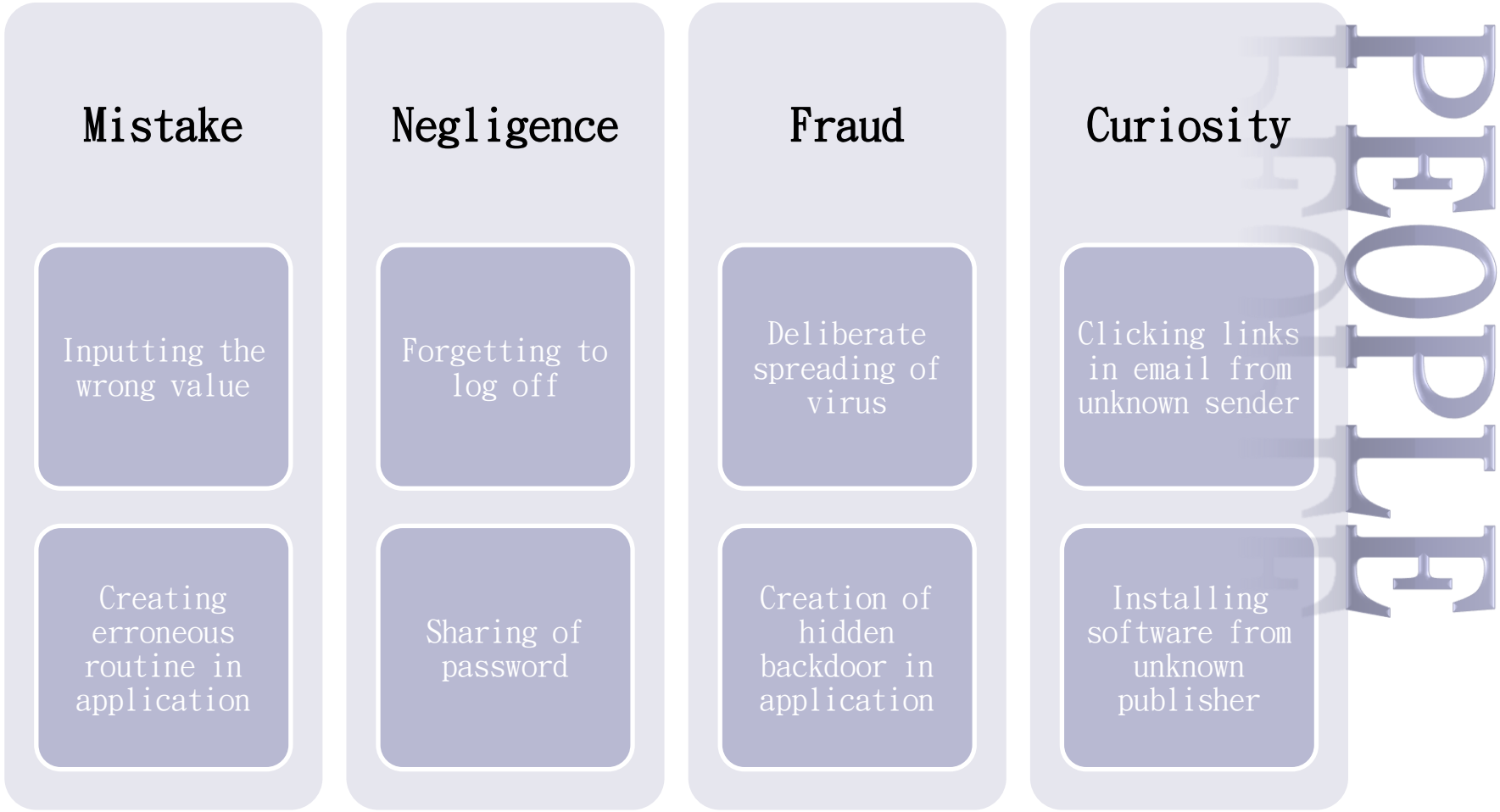
- Technology is fallible
- Organisation may not be able to adequately address all technical security concerns
- Technology is expensive
- **People implement and operate technologies**

PEOPLE- always the weakest link

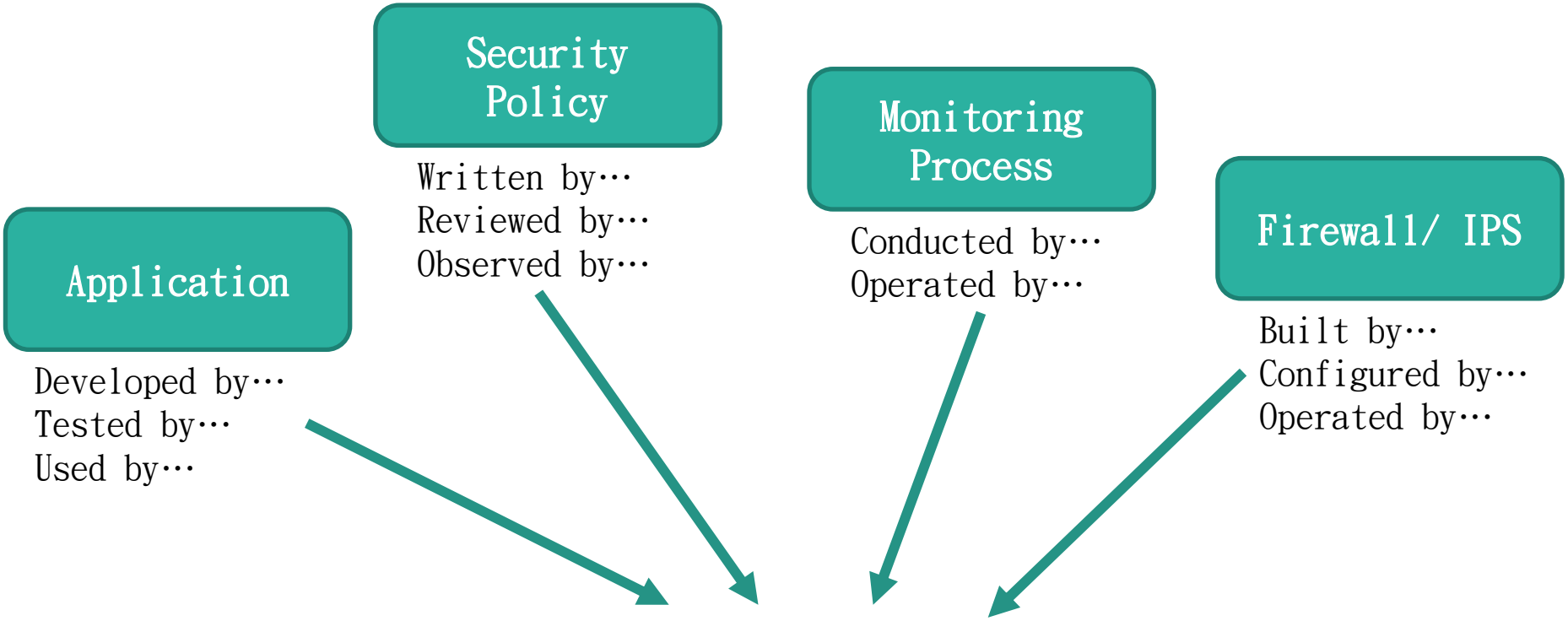
Human Factor- the Risk Management Perspective

- **Threats**- human causing threats.
  E.g. deliberate circumvention of security controls by malicious staff or outsider
- **Vulnerabilities**- human creating the vulnerability in campus.
  E.g. staff giving out sensitive information (social engineering)
- **Impacts**- breaches creating human impacts.
  E.g. decreased trust towards system integrity

Human Factors in Information Security



Human Factors in Information Security



Examples

- Application Authentication
  - Password policy defined with requirements over password length, complexity and expiry
  - Password policy implemented into the application used by general departmental users
  - Validation and expiration reminders implemented to help users in observing the password policy requirements
  - Due to the frequent password change, user wrote the password on a memo and stuck on the screen

Will you hang your key next to your door?

Examples

- System Patch
  - Vendor identified system vulnerabilities
  - System patch and proof-of-concept were announced
  - Patch was not installed by the administrator due to the large amount of security updates available
  - Virus was developed utilising the identified vulnerability
  - Virus outbreak in campus network

Examples

- Malicious Email
  - Security awareness training was conducted to spread that message that email attachment from suspicious senders should not be opened
  - Virus writers managed to find ways to leverage on general users' curiosity by coming up with interesting subject line, body text and file name.

To unsubscribe, click here…

Click to support…

You won a prize!

A funny photo attached…

Your favourite service is coming to end-of-life…

Reset your password…

Love Letter.doc…

Like…

Information Security Roles and Responsibilities

Management

- Understand the importance of information security
- Understand the influence to users for management support towards information security
- Establish general direction and allocate sufficient budget for information security management (including technical and awareness training)
- Follow up on security breaches
- Involve the information security team in management meetings

Information Security Team

- Obtain up-to-date information regarding security trends and latest threats and vulnerabilities
- Conduct adequate security awareness training to users
- Review and update the security policies and communicate changes to users
- Duly report security incidents to management
- Review the technical competence of operation team
- Understand the security trends in campus and identify potential loopholes

Information Security Roles and Responsibilities

Operation Team

- Obtain up-to-date information regarding security trends and latest threats and vulnerabilities
- Acquire up-to-date technical information and system related security updates
- Timely implement security updates to systems and report to the security management team

Users

- Understand their roles in information security
- Attend security awareness training
- Be skeptical when dealing with suspicious emails and Internet contents
- Use a strong password and keep them secret

Management Support

Enforcement of Policy and Procedures

Awareness Training

Mistake → REVIEW PROCESS

Negligence/ Curiosity → AWARENESS

Fraud → SUPERVISION

Q&A

?

Copyright Statement