Joint Universities Computer Centre Limited ("JUCC")

Information Security Awareness Training- Session One

Information Security and Challenges

Agenda

Overview of Information Security Management

- Information Security Concept
- Privacy and Personal Data
- Managing Information Security

Information Security Standard and Policies

- Industry Leading Standards
- Good Information Security Practice in Universities

Challenges for Information Security

- Information Security Challenges in Universities
- Information Security Trends

Overview of Information Security Management

Internet source:

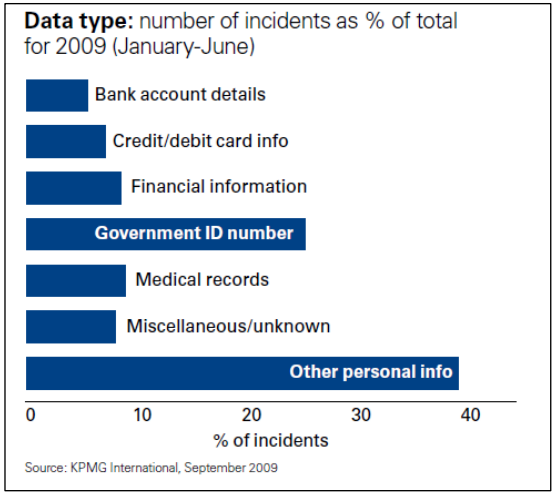
Information security means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction.

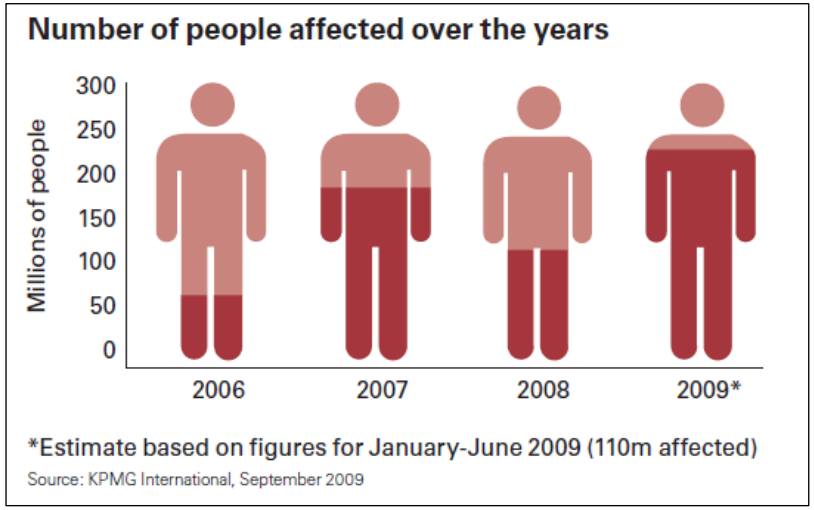
ISO27001:

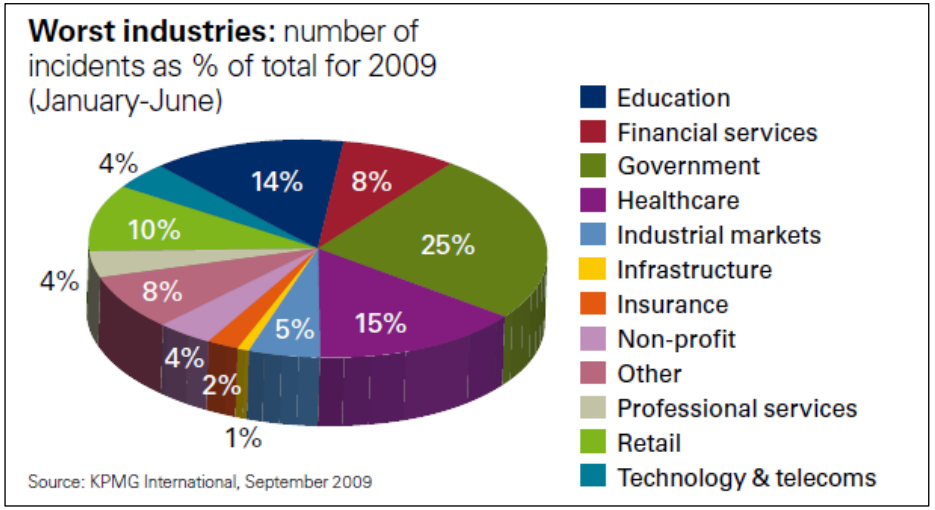
Information security exists to: "ensure adequate and proportionate security controls that adequately protect information assets and give confidence to customers and other interested parties. This can be translated into maintaining and improving competitive edge, cash flow, profitability, legal compliance and commercial image."

Impact of Data Leakage in 2009

"The Education Sector is definitely a key victim of data leakage"







Overview of Information Security Management

Chaminade posted Social Security numbers of thousands of students online

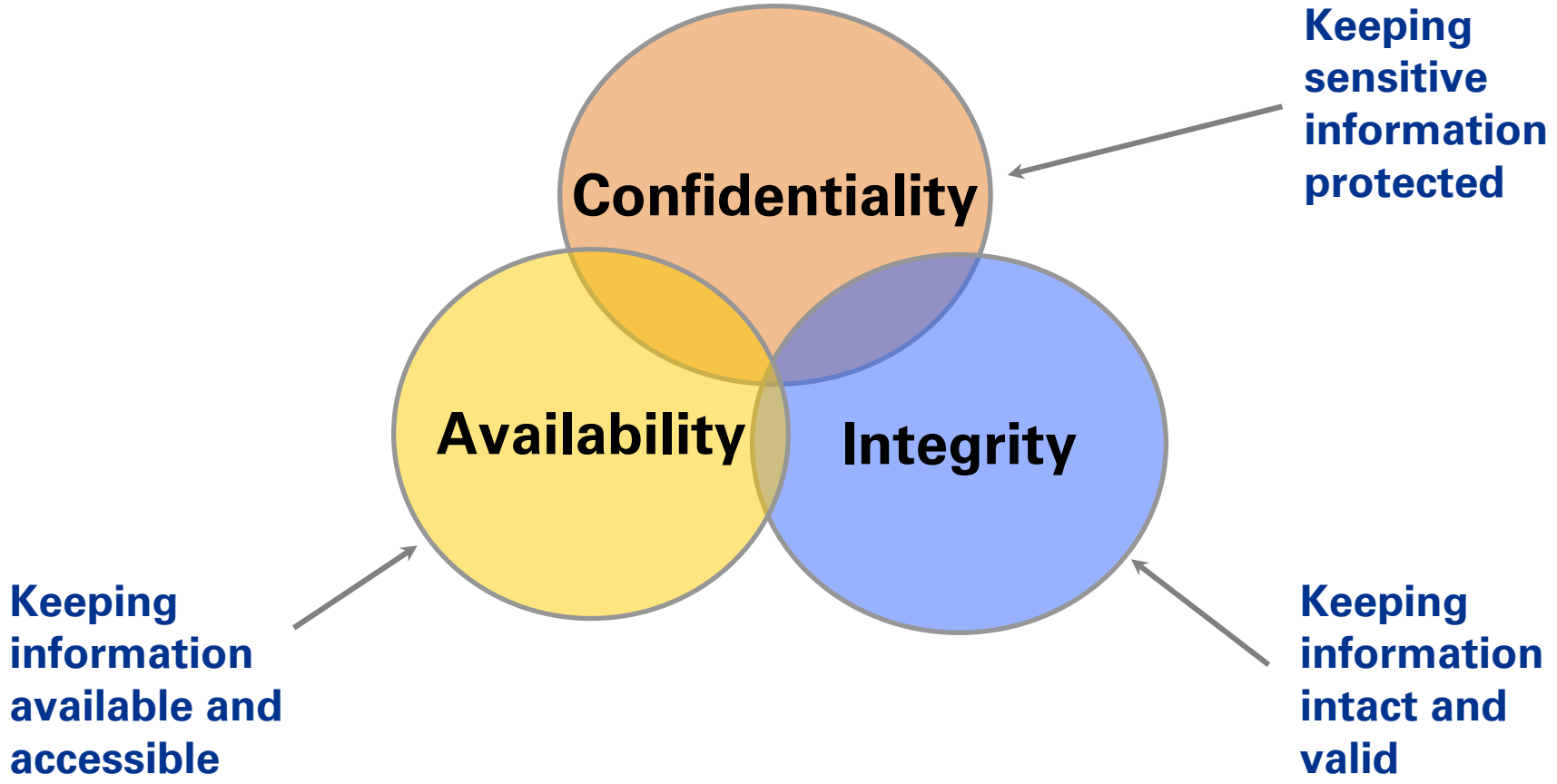
By Star-Bulletin staff

Chaminade University inadvertently **posted confidential information**, including Social Security numbers, of thousands of students, on its **Web site** for months, school officials said today.
An investigation determined the report was placed on obscure -- though publicly accessible -- Web pages because of **human error**, according to a university news release. The information was accessible for about eight months, although there is no evidence of its use, officials said. The university estimates that personally identifiable data for 4,500 students were in the report. Those affected include undergraduate students who attended the university from 1997 to 2006.
Chaminade officials are putting in place procedures designed to prevent a recurrence and will provide **additional training to staff regarding the protection of personal information**, the university said.
The university is contacting the people whose information was put online. Those affected are being asked to monitor and review their credit report.

Source: http://www.starbulletin.com/news/breaking/69438757.htm

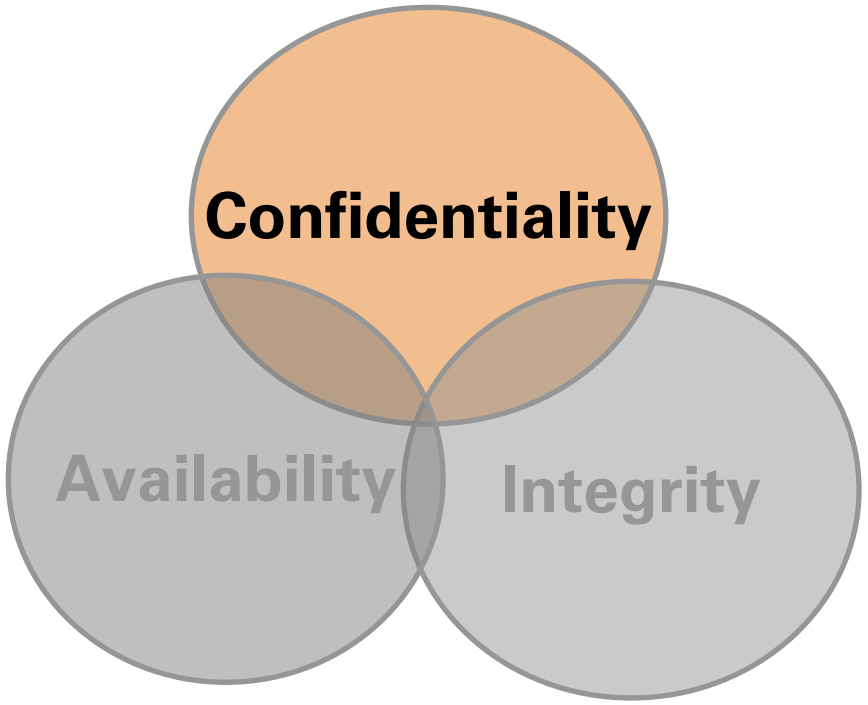
"Data leakage incidents are happening in the universities frequently"

The CIA Concept



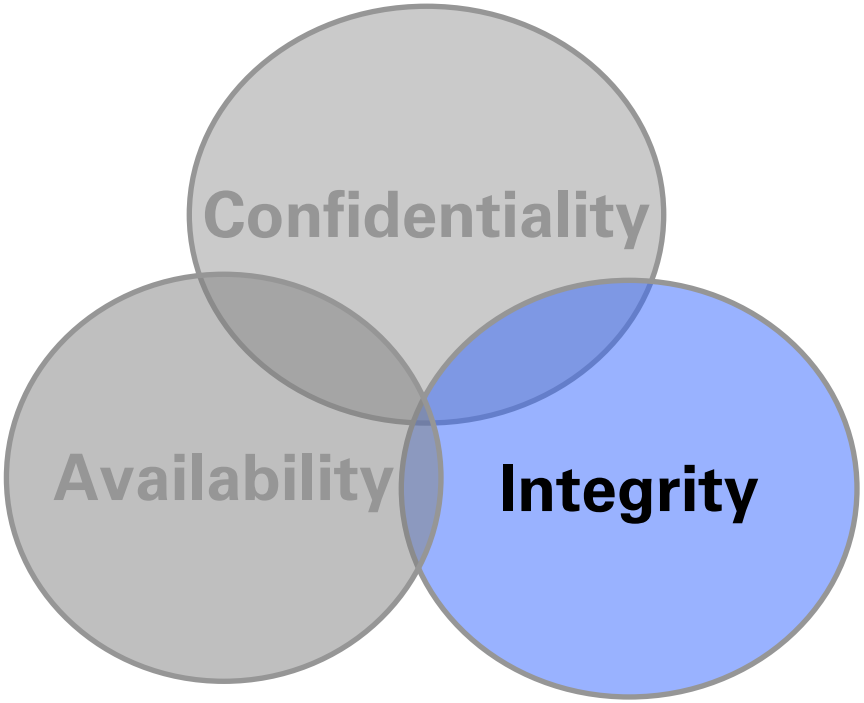
Confidentiality

- Objects are not disclosed to unauthorised subjects.
- Prevent the intentional or unintentional unauthorised disclosure of information.



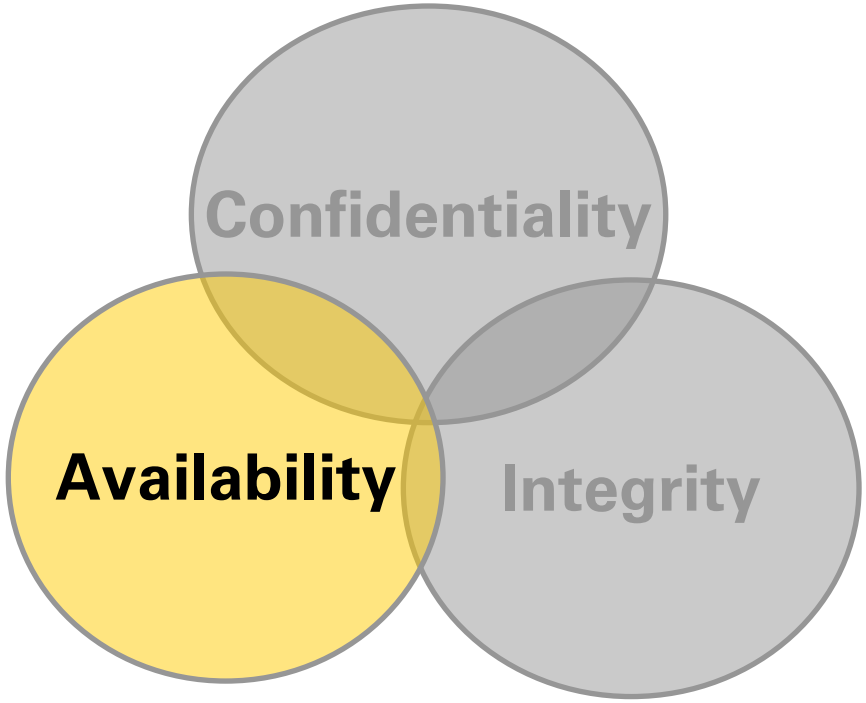
Integrity

- Objects retain their veracity and are only intentionally modified by authorised subjects.
- Systems are free from unauthorised manipulation that will compromise accuracy, completeness, and reliability.
- Data are internally and externally consistent.



Availability

- Authorised subjects are granted timely and uninterrupted access to objects.
- Ongoing availability ensures the reliable and timely access to data or computing resources by the appropriate personnel.



Information Security Concept

Authentication

- The testing or reconciliation of evidence of a user's identity. Users claim their identities to a system.
- Establishes the user's identity and ensures that the users are who they say they are.

Authorisation

- The rights and permissions granted to an individual or process which enable access to information or information resource.

Accountability

- Ability to determine the action and behaviour taken by a single individual.
- Audit trails and logs support accountability.

Privacy and Personal Data

Privacy

The ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively.

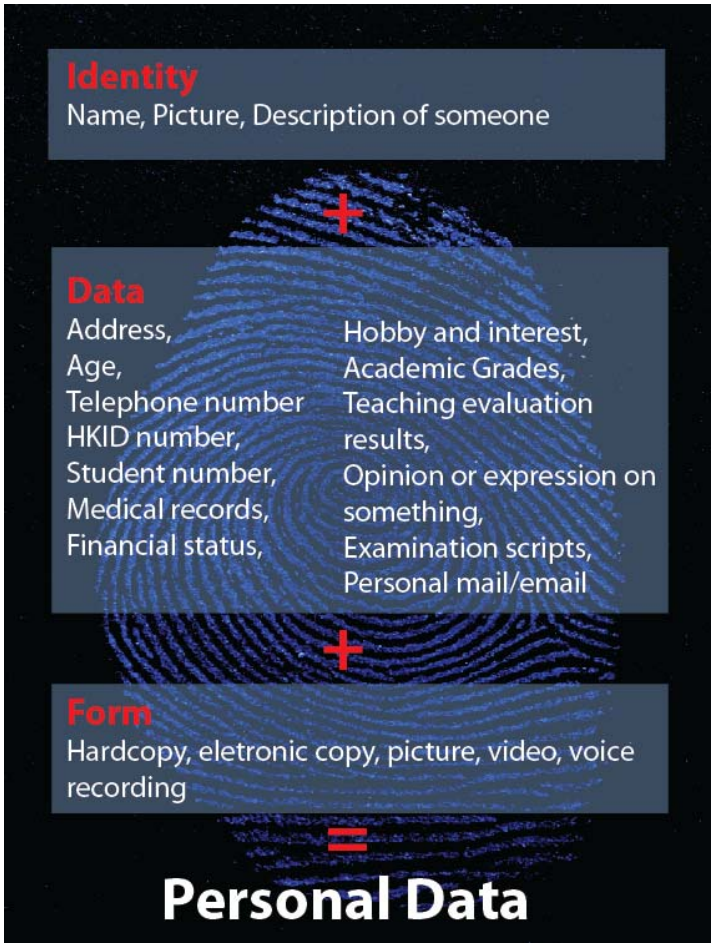
Personal Data (Privacy) Ordinance of Hong Kong

All information about a living, identifiable individual is personal data

(a) from which it is practicable for the identity of the individual to be directly or indirectly ascertained;

(b) relating directly or indirectly to a living individual; and

(c) in a form in which access to or processing of the data is practicable



Data Protection Principles

Principle 1 -- Purpose and manner of collection

Principle 2 -- Accuracy and duration of retention

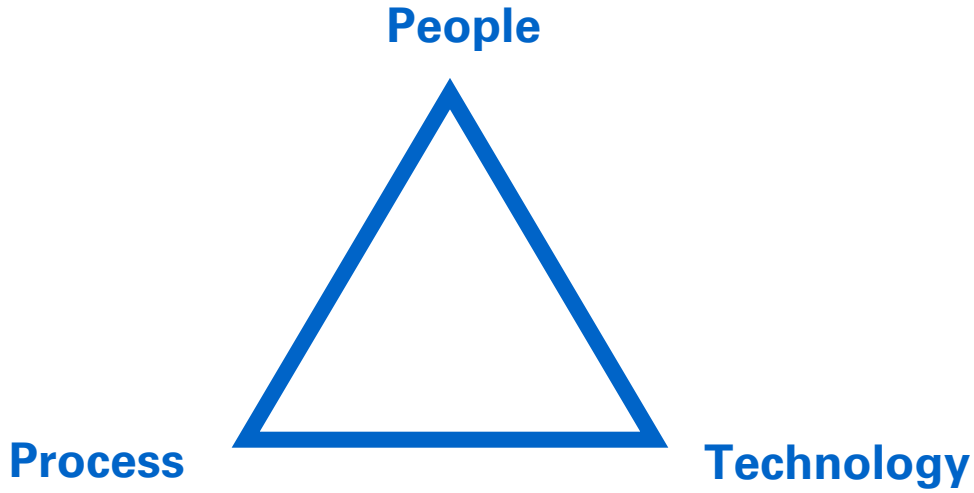
Principle 3 -- Use of personal data

Principle 4 -- Security of personal data

Principle 5 -- Information to be generally available

Principle 6 -- Access to personal data

Managing Information Security



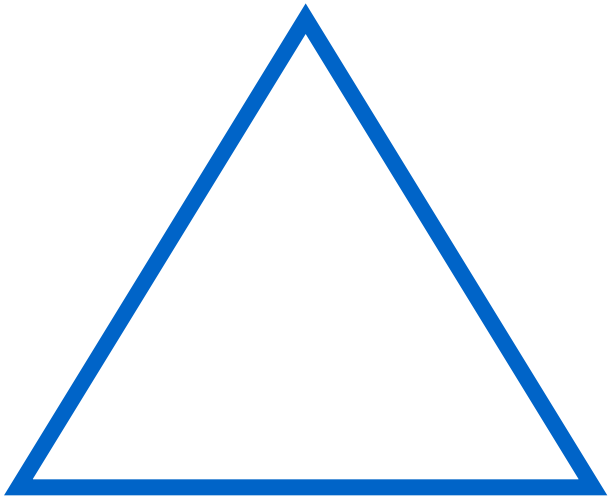
- **Information security is not only related to computer systems.**
- **People is always the weakest link.**
- **A complete framework is required to manage information security.**

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

Managing Information Security

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

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

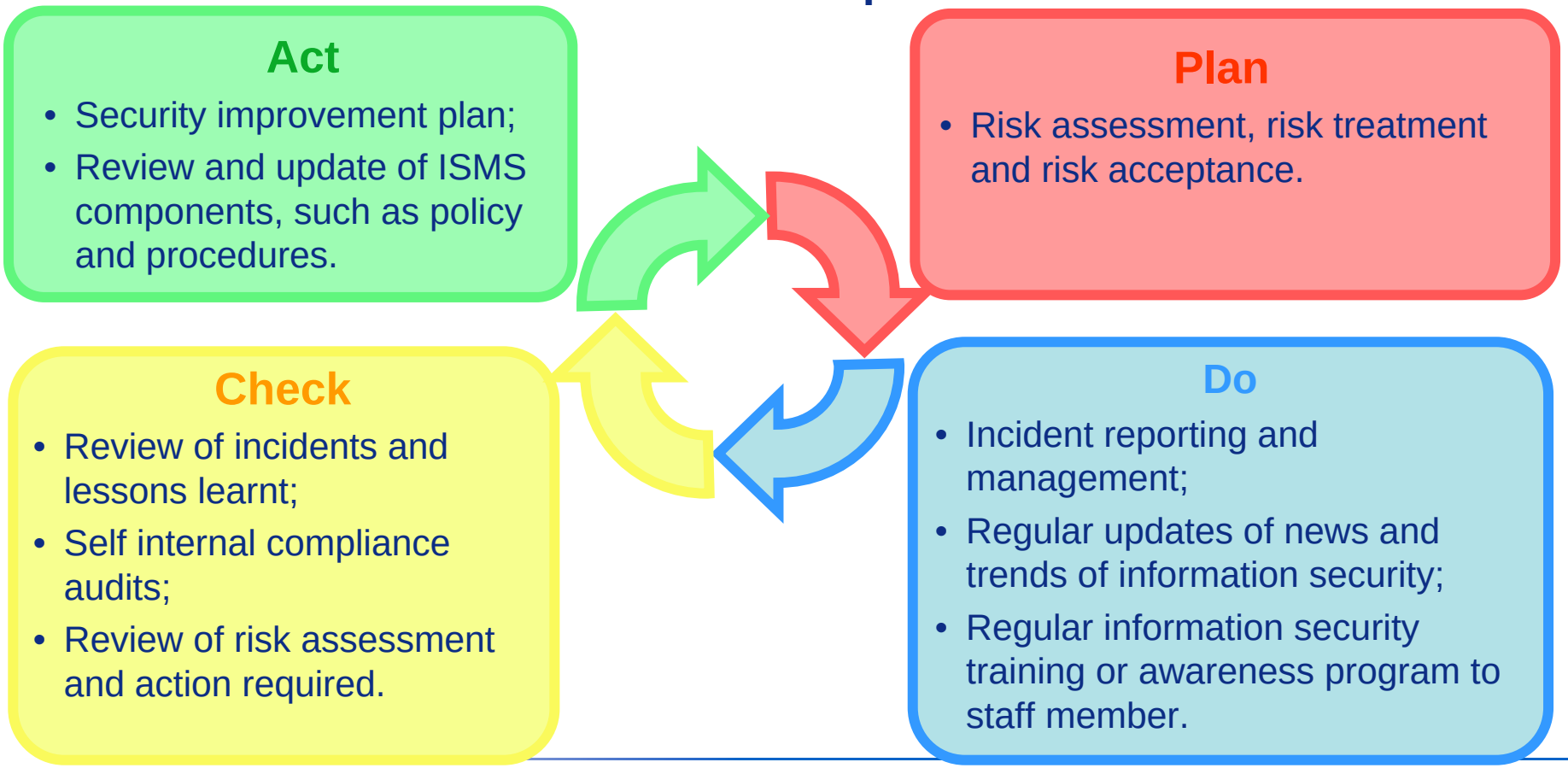


Technology
- Antivirus
- Firewall
- Intrusion Detection System
- Security patches
- Security logging

Plan-Do-Check-Act (PDCA)

A model adopted by ISO27001

A PDCA example



Industry standard for managing information security

- **ISO Standards**
  - ISO/IEC 27001:2005 (Information Security Management System)
  - ISO/IEC 27002:2005 (Code of Practice for Information Security Management)
  - ISO/IEC 15408 (Evaluation Criteria for IT Security)
  - ISO/IEC 13335 (IT Security Management)
- **COBIT**
- **ITIL (ISO/IEC 20000 Series)**

ISO 27001 - Information Security Management System

- ISO 27001 is the International Standard for Information Security Management.
- It specifies the requirements of an Information Security Management System (ISMS).
- ISMS addresses the management of information security within the context of the organisation's overall business risk.
- Management responsibility – commitment, resources and training.
- Plan-Do-Check-Act (PDCA) life cycle model is a key component of ISO27001 in the ISMS implementation.
- ISMS is widely adopted by various organisations around the world, including universities such as Georgia State University and the University of Leeds.

ISO 27001 addresses the following 11 domains

- Security Policy
- Organisation of Information Security
- Asset Management
- Human Resource Security
- Physical and Environmental Security
- Communication and Operations Management
- Access Control
- Information System Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Good Information Security Practice in Universities

For IT Professional & Administrative Personnel

User Account/Access Administration:

- User accounts and strong password controls.
- Classify data and create data ownerships.
- Segregation of duties.
- Conducting security awareness training.

Logical Access Controls:

- Identity and access management policies.
- Implement strong password policies and configurations.
- Restrictions and policy on the use of privileged/administrator accounts.

Network Security:

- Installation of devices such as firewall and Intrusion Detection System.
- Periodic firewall log review.
- Perform periodic scanning on network and computers.

Environmental Controls:

- Air conditioning.
- Humidity controls.
- Fire suppression system.
- Raised flooring as a precaution against flooding.

Physical Access Controls & Procedures:

- Security guards.
- Swipe card/biometrically controlled access points.
- Access control lists.
- Perimeter controls.

Incident Management

- Escalation procedures.
- Investigation procedures.
- Defined roles and responsibilities.

Information Security Awareness:

- Regular information Security Awareness Training.

Good Information Security Practice in Universities

For General Users

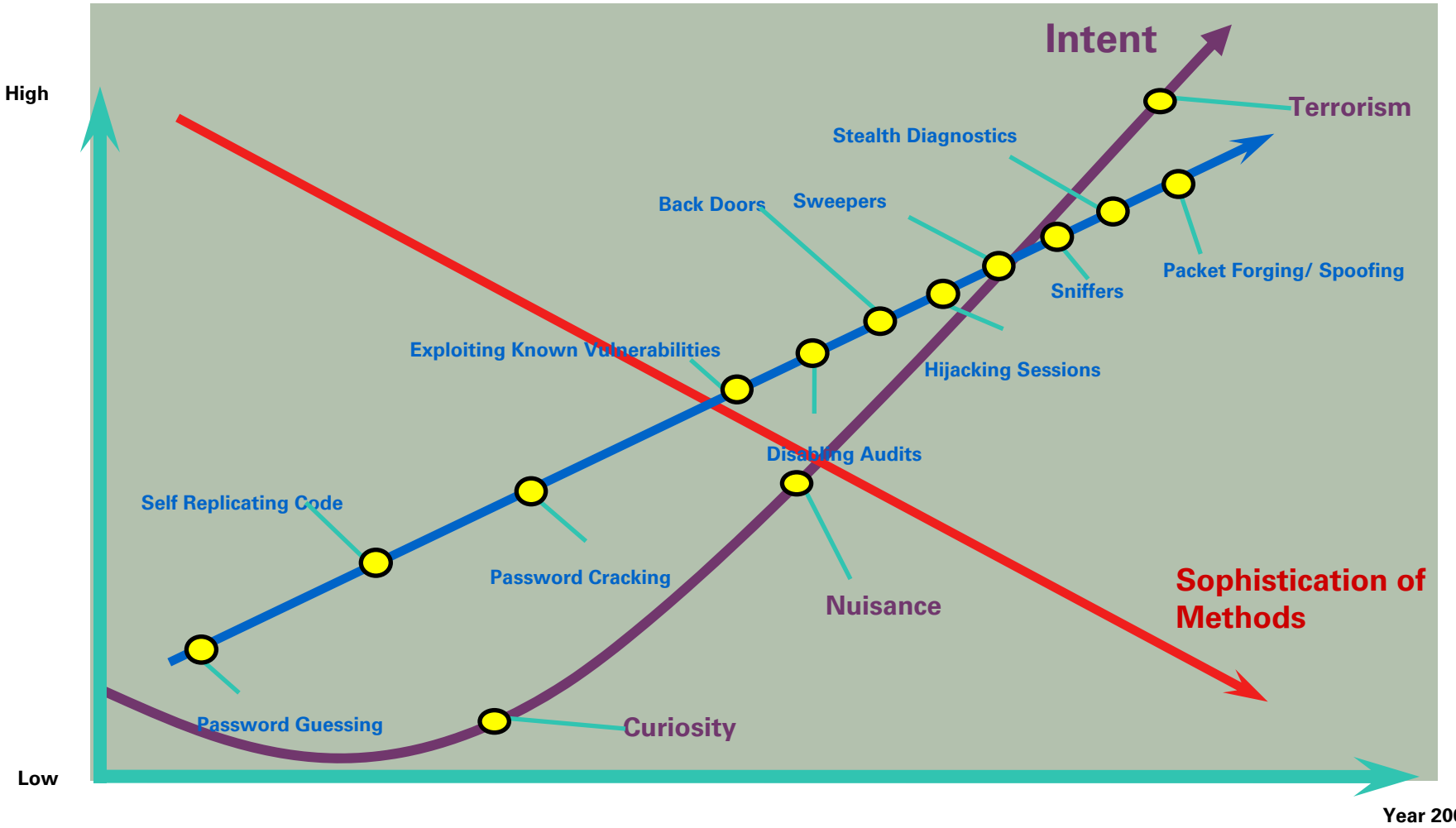
Ten things to be remembered

1. Do not disclose your personal information unless absolutely necessary.
2. Do not provide personal information to untrusted websites
3. Dispose sensitive information with care (e.g. credit card receipts, bank statements)
4. Log out or lock your computer session when left unattended
5. Always encrypt sensitive information in transit and send the decryption key to the recipient separately
6. Do not keep sensitive information in portable storage devices
7. Use anti-virus and anti-spyware in your computer
8. Do not process/enter sensitive data in untrusted computers such as Internet Cafe
9. Be sceptical, consult your IT helpdesk if in doubt
10. Remind your colleagues and friends of these 10 things

Information Security Challenges in Universities

- Decentralised management of information resources
- Enormous amount of sensitive and personal data
- Demand of academic freedom makes IS control implementation difficult
- Challenges in raising security awareness of academic staff and students
- Popular hacking targets
- Management commitment is critical
- Lack of resources

Information Security Trends



Information Security Trends

Technology	Trends
Virtualisation	• Preventing infections from cross pollinating between virtual machines • Adoption of virtualisation technology for disaster recovery
Cloud Computing	• Information protection in the public network • Data confidentiality in external systems
Analytical filtering ruleset	• Content analysis and filtering instead of network level filtering • Prevention of sensitive data leakage through campus network
Portable Media	• User awareness in protecting data in portable media • Use of encrypted media • Erasing / wiping sensitive data after used
IT Outsourcing	• Data confidentiality in outsourced IT operations • Business continuity collaboration with IT service providers

Information Security Trends

Technology	Trends
Web 2.0	• Application security in adopting Web 2.0 technologies • Source code security review
Peer to peer data sharing	• User awareness in not sharing copy-righted or confidential materials • Network traffic shaping
Social web site	• Sensitive information leakage through social web sites • Identity / data theft • Virus / Trojan infections

Summary

Information Security Concepts

- CIA | 6DPPs | People-Process-Technology | PDCA

- **Privacy & Personal Data**
- **Managing Information Security**
- **Standards & Policies**
- **Good Practice**
- **Challenges**
- **Latest Trend**

Q&A

?