Lecture 1

Introduction to Information Security

UNIVERSITY
OF
JOHANNESBURG

Objectives

- Define information security
- Define key terms and critical concepts of information security
- Describe the information security roles of professionals within an organization

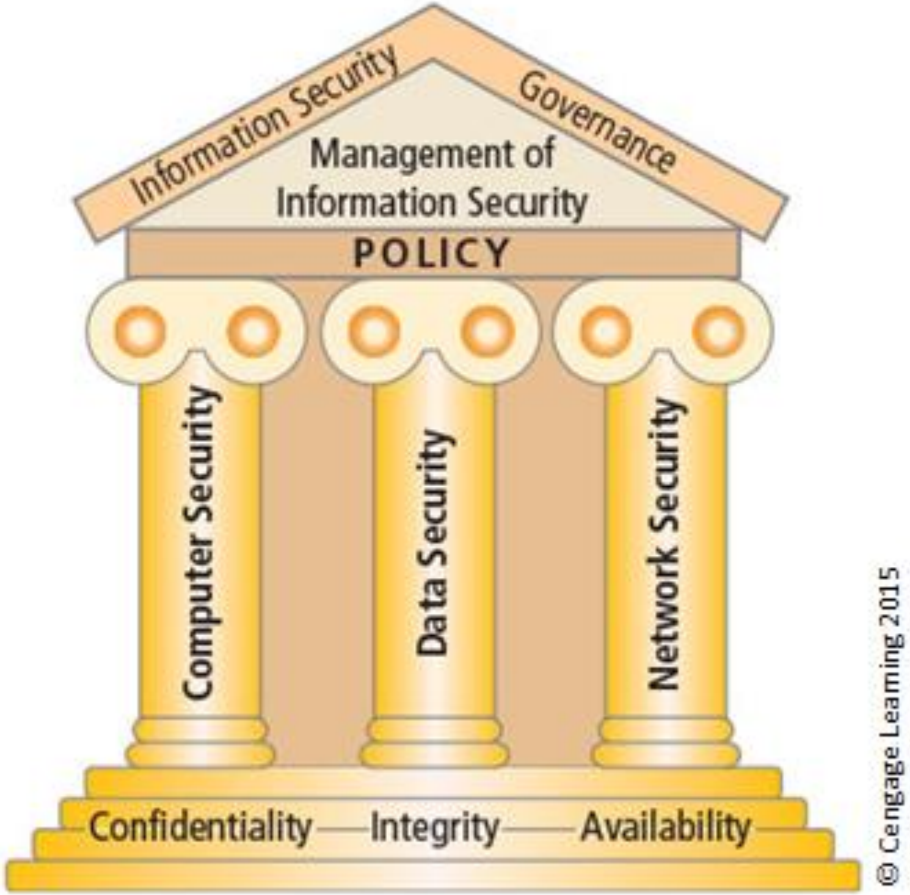
What Is Security? (1 of 2)

- “A state of being secure and free from danger or harm; the actions taken to make someone or something secure.”
- A successful organization should have multiple layers of security in place to protect:
  - Operations
  - Physical infrastructure
  - People
  - Functions
  - Communications
  - Information

What Is Security? (2 of 2)

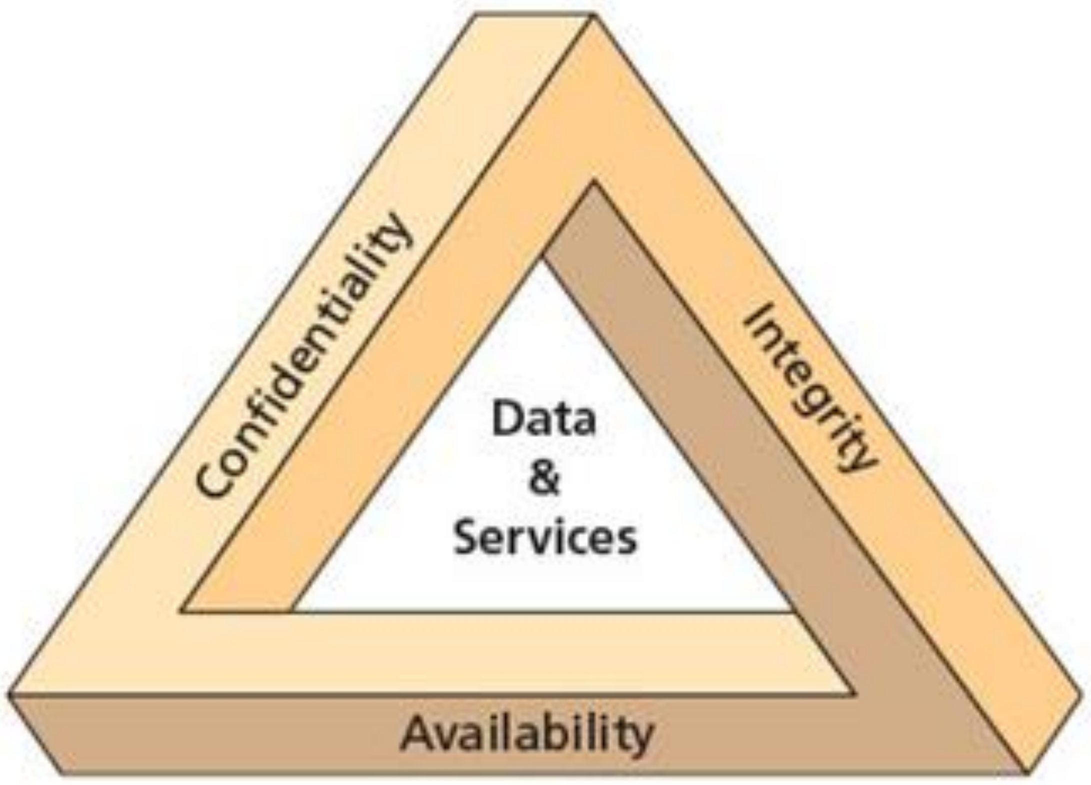
- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Includes information security management, data security, and network security
- C.I.A. triad
  - Is a standard based on confidentiality, integrity, and availability, now viewed as inadequate.
  - Expanded model consists of a list of critical characteristics of information.

Figure 1-5 Components of information security (1 of 2)



© Cengage Learning 2015

Figure 1-5 The C.I.A. triad (2 of 2)



© Cengage Learning 2015

Key Information Security Concepts (1 of 3)

- Access
- Asset
- Attack
- Control, safeguard, or countermeasure
- Exploit
- Exposure
- Loss
- Protection profile or security posture

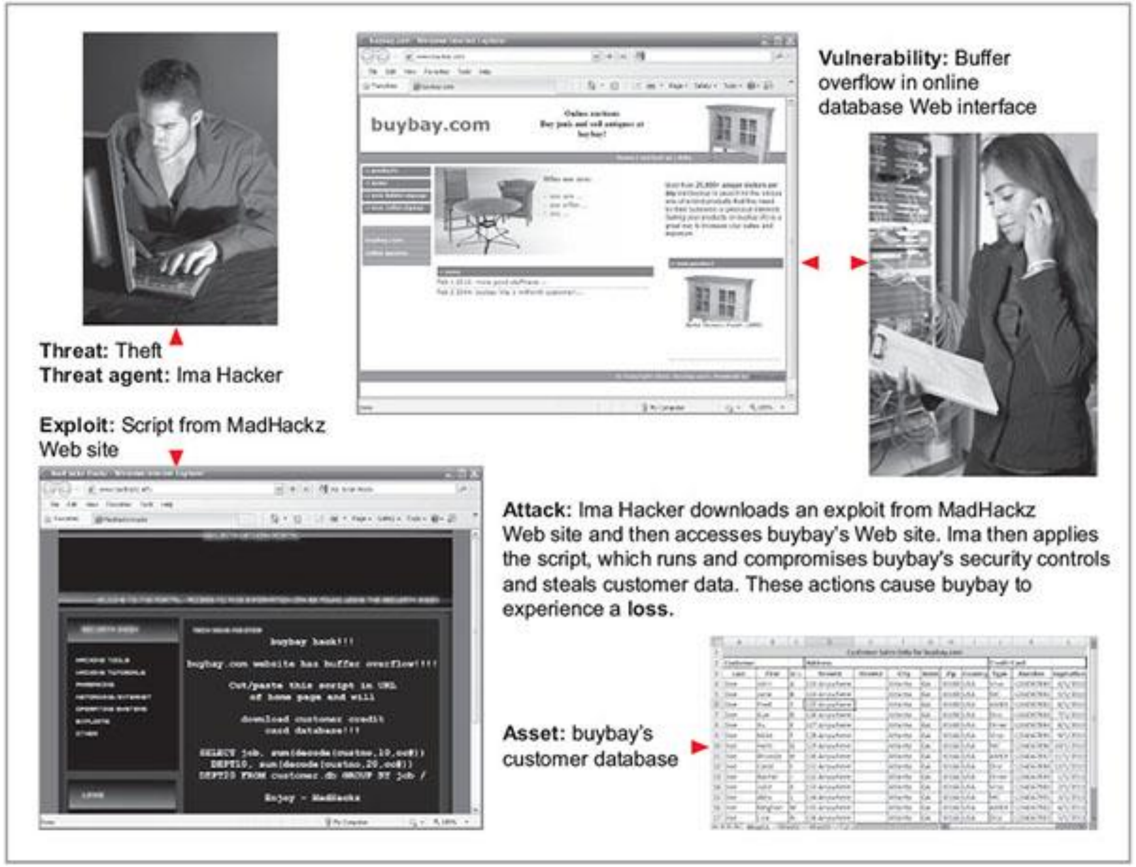
Key Information Security Concepts (2 of 3)

- Risk
- Subjects and objects of attack
- Threat
- Threat agent
- Threat event
- Threat source
- Vulnerability

Key Information Security Concepts (3 of 3)

- A computer can be the subject of an attack and/or the object of an attack.
  - When it is the subject of an attack, the computer is used as an active tool to conduct attack.
  - When it is the object of an attack, the computer is the entity being attacked.

Figure 1-7 Key concepts in information security



Vulnerability: Buffer overflow in online database Web interface

Threat: Theft
Threat agent: Ima Hacker

Exploit: Script from MadHackz Web site

Attack: Ima Hacker downloads an exploit from MadHackz Web site and then accesses buybay's Web site. Ima then applies the script, which runs and compromises buybay's security controls and steals customer data. These actions cause buybay to experience a **loss.**

Asset: buybay's customer database

```
buybay hack!!!

buybay.com website has buffer overflow!!!!

Cut/paste this script in URL
of home page and will

download customer credit
card database!!!

SELECT job, sum(decode(custno,10,cc#))
DEPT10, sum(decode(custno,20,cc#))
DEPT20 FROM customer.db GROUP BY job /

Enjoy - MadHackz
```

Source. (top left to bottom right): © iStockphoto/tadija, Internet Explorer, © iStockphoto/darrenwise , Internet Explorer, Microsoft Excel.

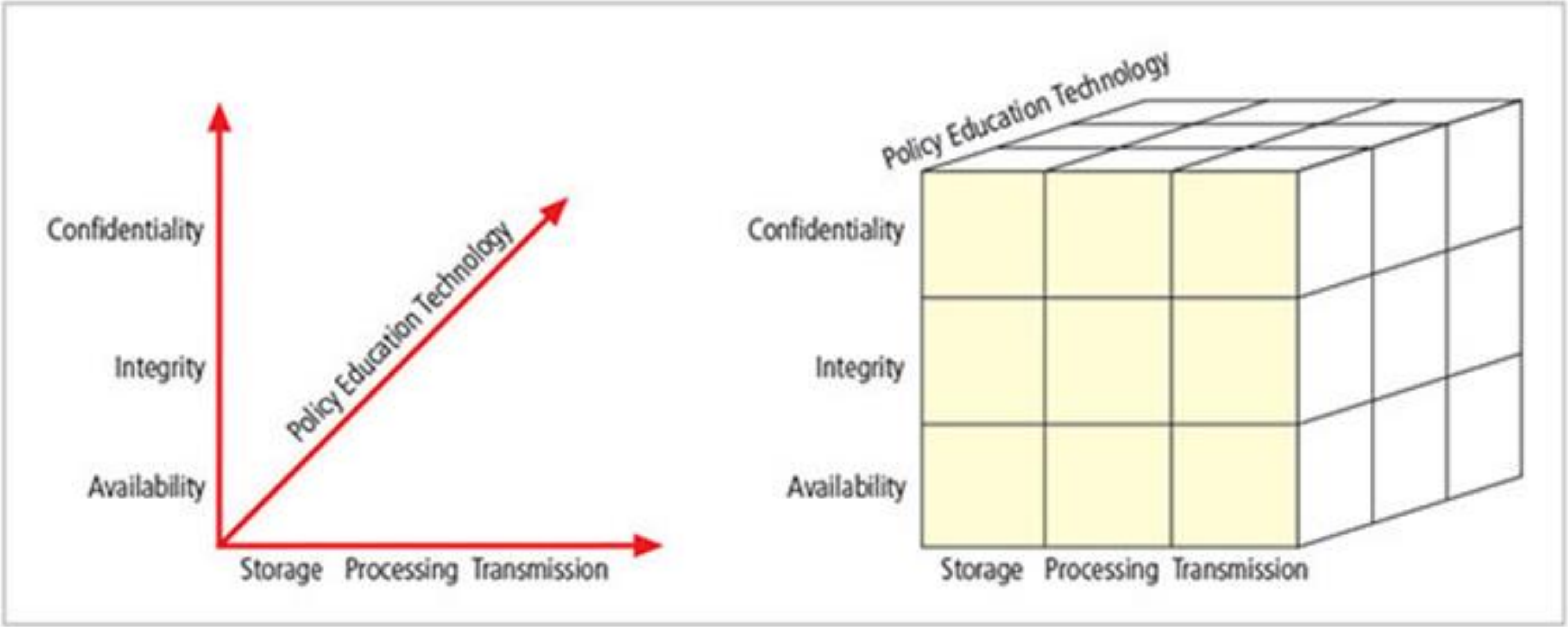
Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - Availability
  - Accuracy
  - Authenticity
  - Confidentiality
  - Integrity
  - Utility
  - Possession

ISO 7498/2 Information Security Services

- Identification and Authentication
- Authorisation
- Integrity
- Confidentiality
- Non-repudiation \ Non-denial

Figure 1-9 The McCumber Cube



© Cengage Learning 2015

Components of an Information System

- Information system (IS) is the entire set of people, procedures, and technology that enable business to use information.
  - Software
  - Hardware
  - Data
  - People
  - Procedures
  - Networks

Balancing Information Security and Access

- Impossible to obtain perfect information security—it is a process, not a goal.
- Security should be considered a balance between protection and availability.
- To achieve balance, the level of security must allow reasonable access, yet protect against threats.

Approaches to Information Security Implementation: Bottom-Up Approach

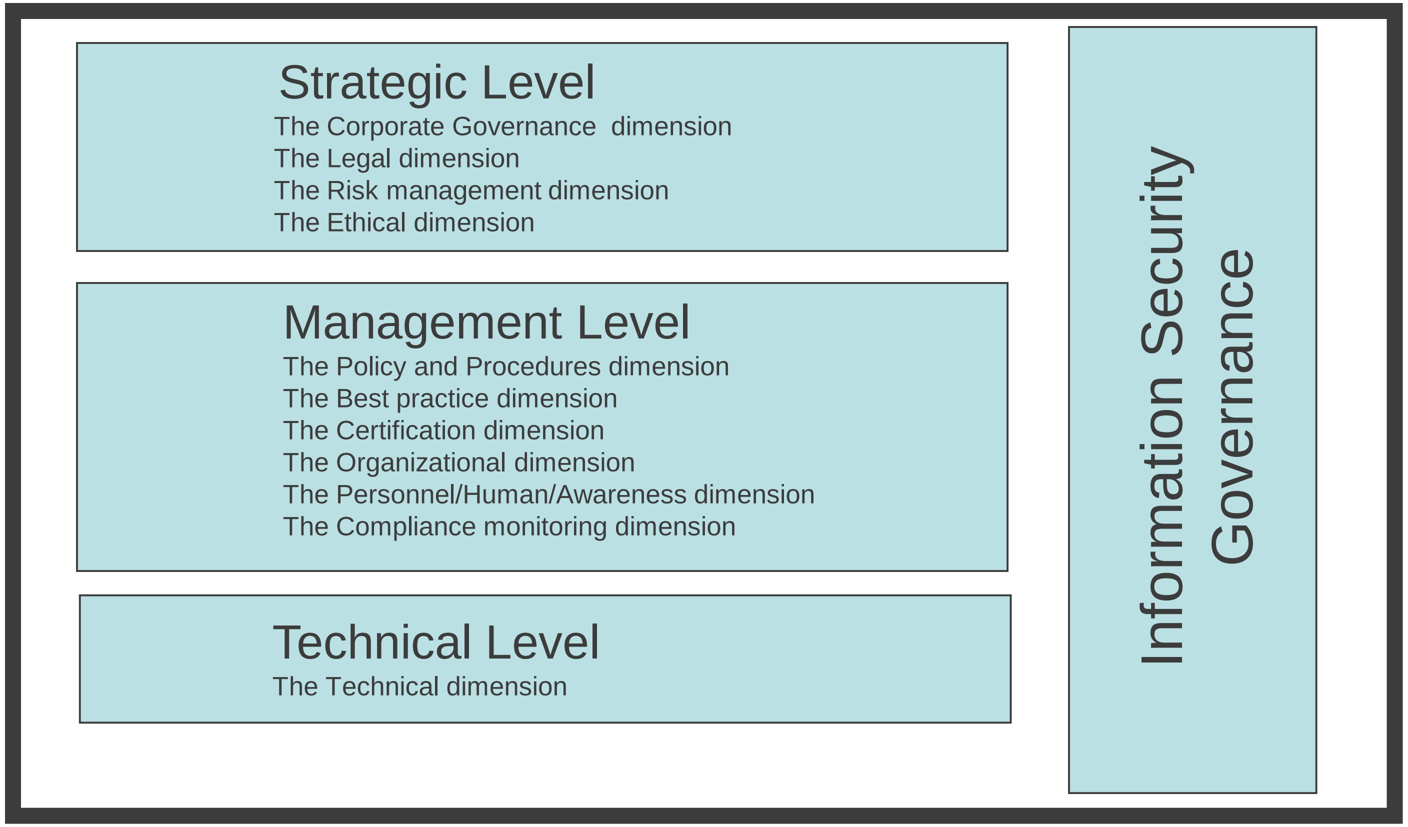
- Grassroots effort: Systems administrators attempt to improve security of their systems.
- Key advantage: technical expertise of individual administrators
- Seldom works, as it lacks a number of critical features:
  - Participant support
  - Organizational staying power

Approaches to Information Security Implementation: Top-Down Approach

- Initiated by upper management
  - Issue policy, procedures, and processes
  - Dictate goals and expected outcomes of project
  - Determine accountability for each required action
- The most successful type of top-down approach also involves a formal development strategy referred to as systems development life cycle.

Modern information security is a multidimensional discipline

An Information Security Plan



Strategic Level

The Corporate Governance dimension
The Legal dimension
The Risk management dimension
The Ethical dimension

Management Level

The Policy and Procedures dimension
The Best practice dimension
The Certification dimension
The Organizational dimension
The Personnel/Human/Awareness dimension
The Compliance monitoring dimension

Technical Level

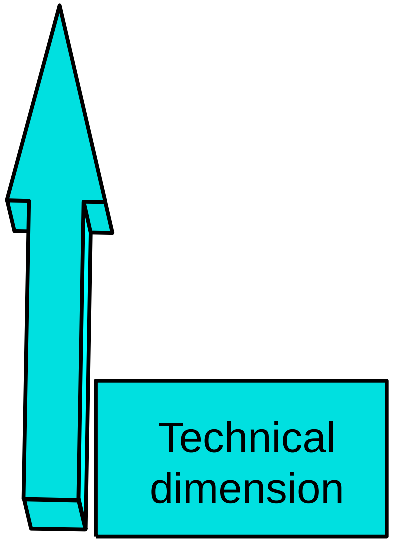
The Technical dimension

Information Security Governance

The interdependence of the dimensions

'If I can get my infrastructure secure, I will be happy'

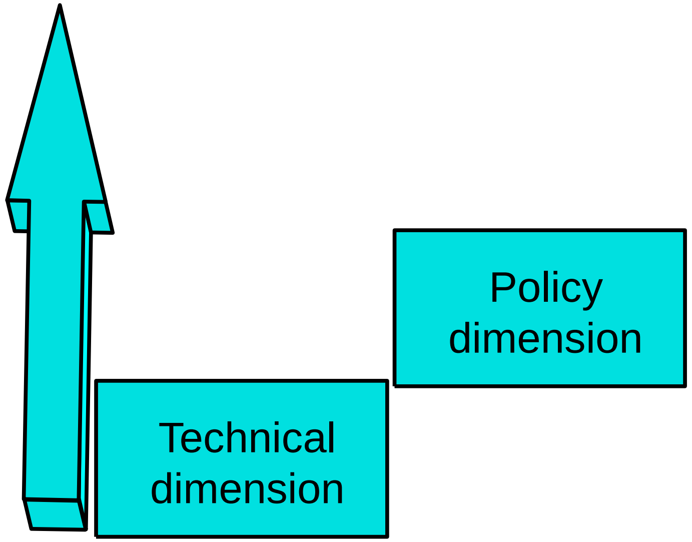
- Enter the : **Technical dimension** of information security (logical access control, firewalls, anti-virus software etc)



The interdependence of the dimensions

'I have installed logical access control, and but I must now configure it. What access rights should employees have?'

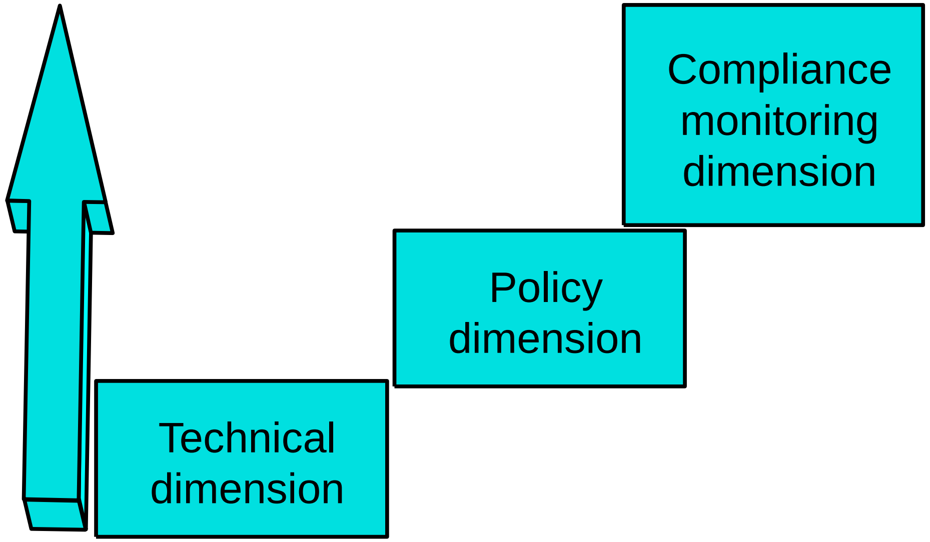
- Enter the : **Policy dimension** of information security



The interdependence of the dimensions

'How do I know there is compliance to my policies?'

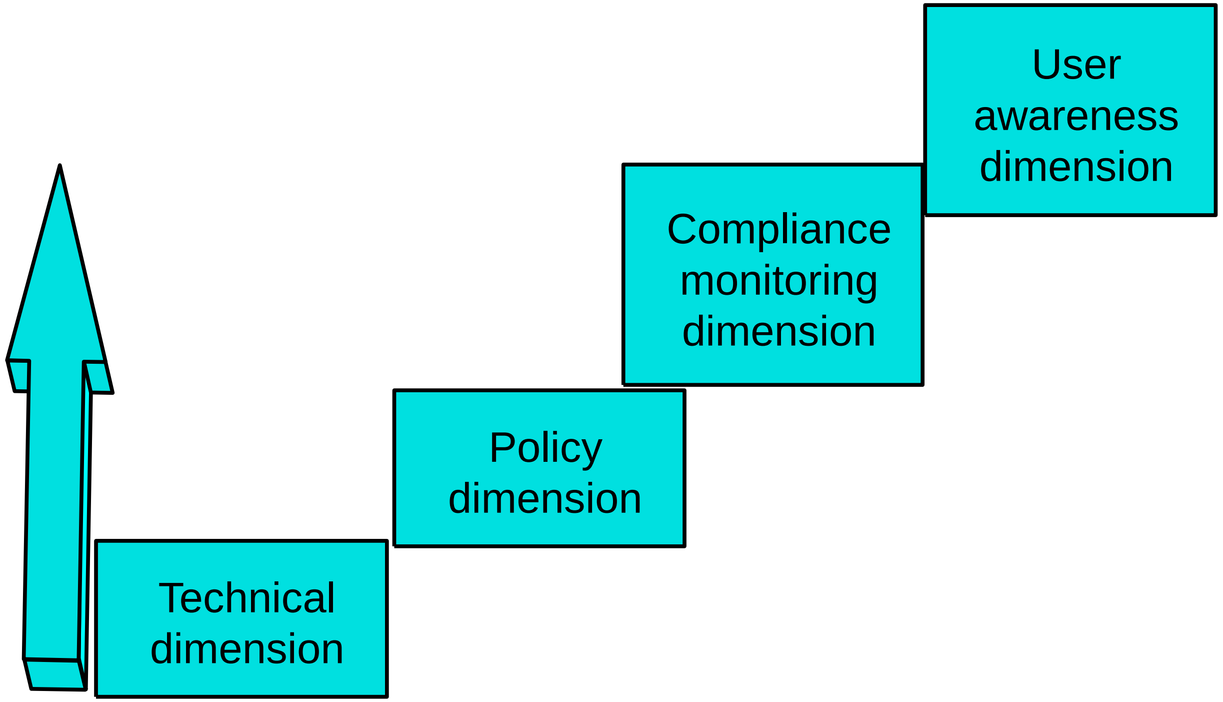
- Enter the : **Compliance Measuring/Monitoring/ real time auditing dimension** of information security



The interdependence of the dimensions

'Employees are not complying because they are ignorant about the policies'

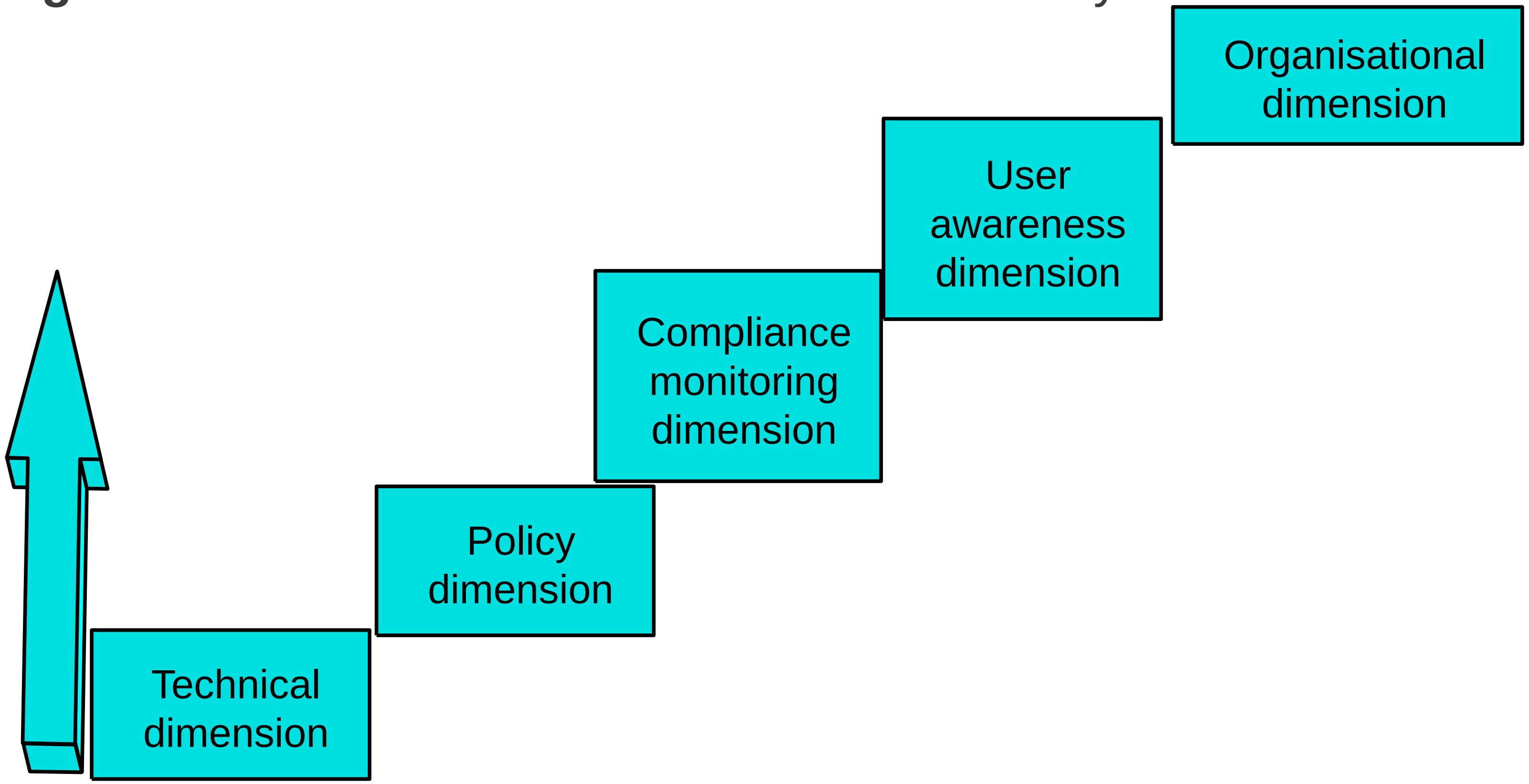
- Enter the : **User Awareness dimension** of information security



The interdependence of the dimensions

'To whom must the user reports incidents?'

- Enter the : **Organisational dimension** of information security



Technical dimension

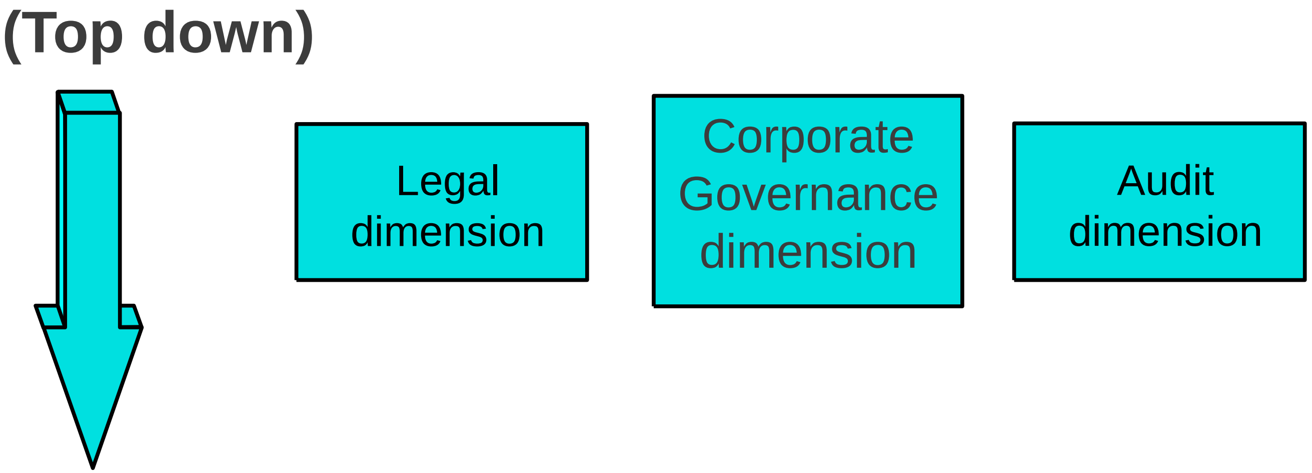
Policy dimension

Compliance monitoring dimension

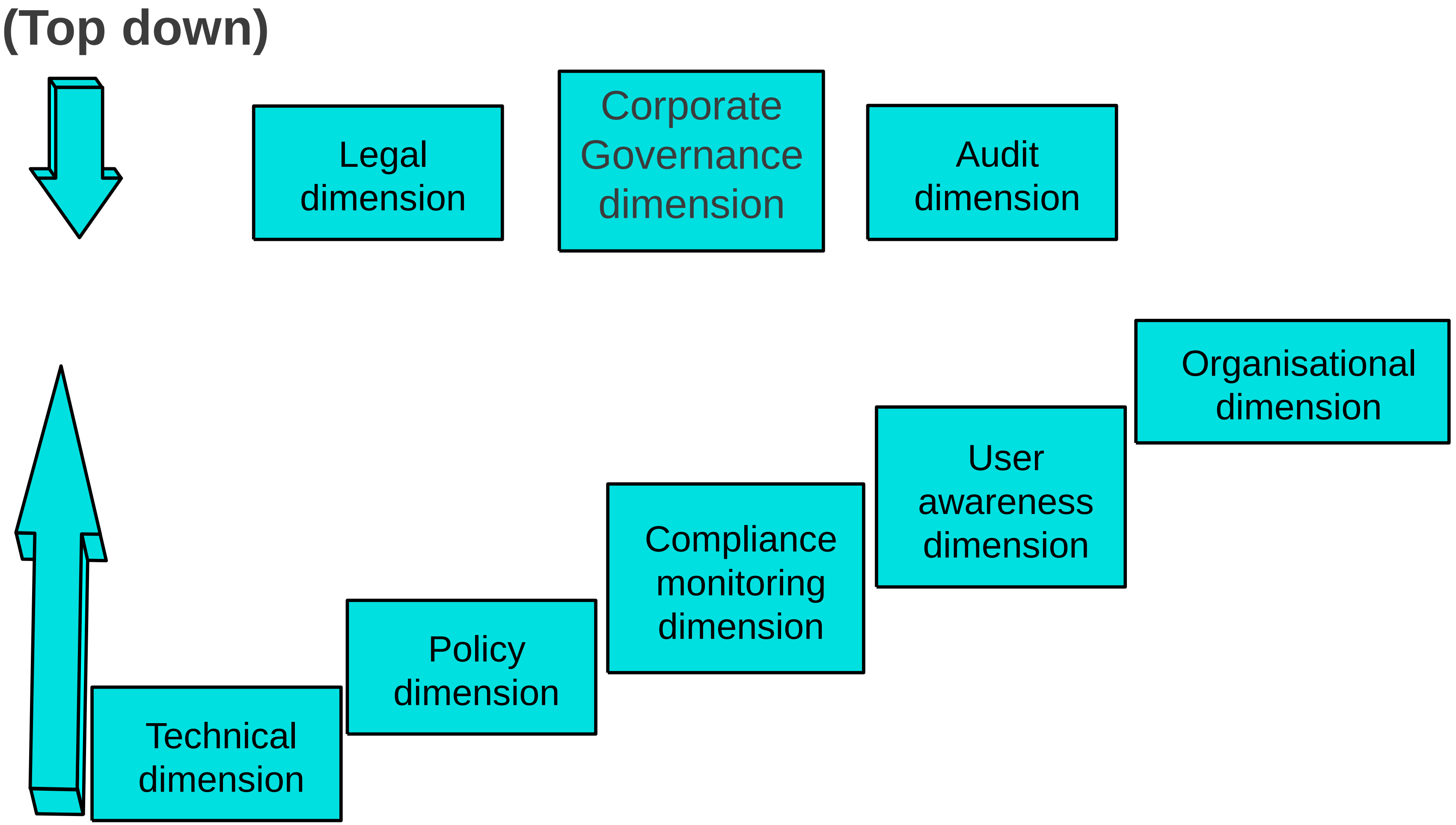
User awareness dimension

Organisational dimension

The interdependence of the dimensions



Multidimensional two directional approach to Information Security



(Top down)

Legal dimension

Corporate Governance dimension

Audit dimension

Technical dimension

Policy dimension

Compliance monitoring dimension

User awareness dimension

Organisational dimension

Security Professionals and the Organization

- Wide range of professionals are required to support a diverse information security **program**.
- Senior management is the key component.
- Additional administrative support and technical expertise are required to implement details of the IS program.

Senior Management

- Chief information officer (CIO)
  - Senior technology officer
  - Primarily responsible for advising the senior executives on strategic planning
- Chief information security officer (CISO)
  - Has primary responsibility for assessment, management, and implementation of IS in the organization
  - Usually reports directly to the CIO

Information Security Project Team

- A small functional team of people who are experienced in one or multiple facets of required technical and nontechnical areas:
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users

Data Responsibilities

- Data owners: senior management responsible for the security and use of a particular set of information
- Data custodians: responsible for the information and systems that process, transmit, and store it
- Data users: individuals with an information security role

Communities of Interest

- Group of individuals united by similar interests/values within an organization
    - Information security management and professionals
    - Information technology management and professionals
    - Organizational management and professionals

Summary

- Information security is the protection of assets that use, store or transmit information.
- Information security is not just technology, but involves multiple domains.
- Information security is a balancing act between security and access.
- There is a bottom-up and top-down approach to implement information security.
- ISO 7498/2 lists five information security services that can be addressed using technology.
- There are many role players in information security programs.