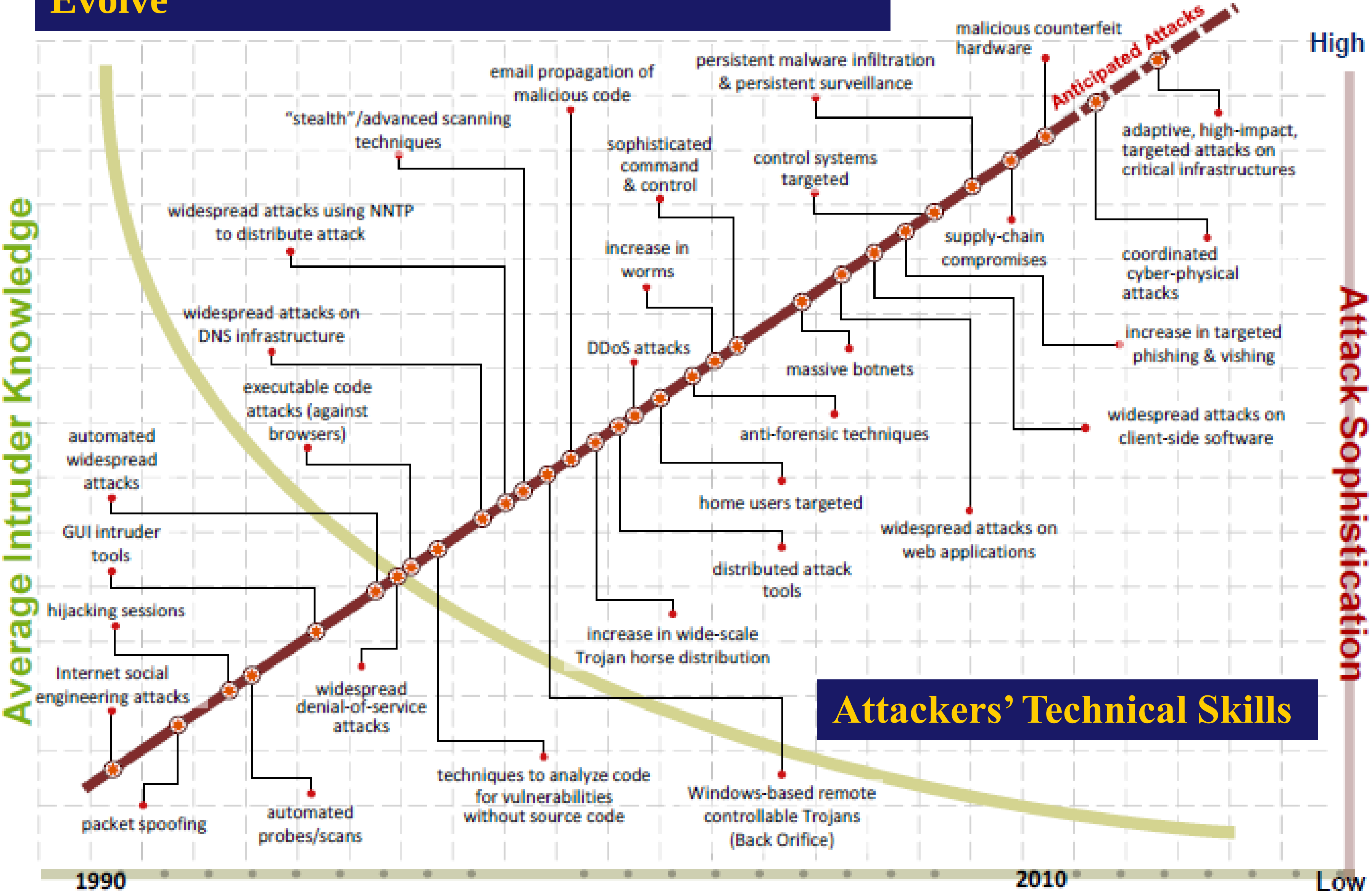
INTRODUCTION TO SECURITY MANAGEMENT

Introduction

- **Information Technology** is critical to today's business and society
  - enables the storage and transportation of information from one business unit to another
- What if it fails?
  - even only for a little while?

Cyber Attack Sophistication Continues To Evolve

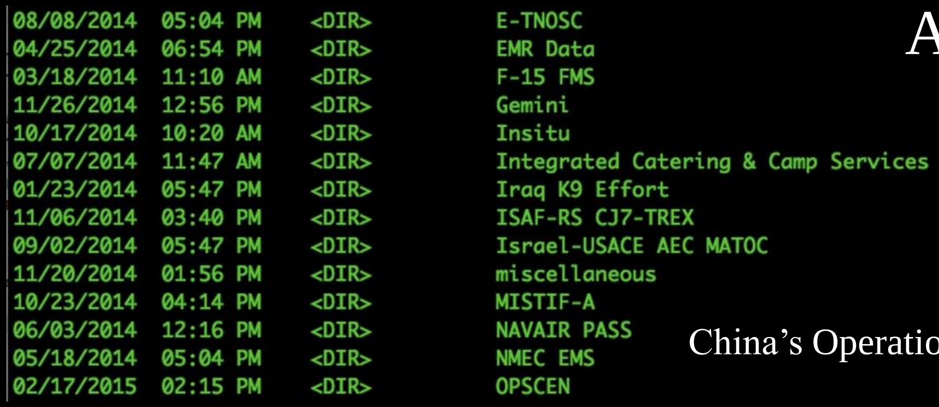


"Cybercrime has become a $105B business that now surpasses the value of the illegal drug trade worldwide." - McAfee CEO, 2007

"The 2015 Anthem data breach cost over $100 million, according to ZDNet.com, with some estimating $8 to $16 billion."

"Over 21M comprehensive personnel files was stored with an estimated 5.6M fingerprints compromised in the Office of Personnel and Management (OPM) data breach" … which was "possibly part of larger Advanced Persistent Threat (APT)"

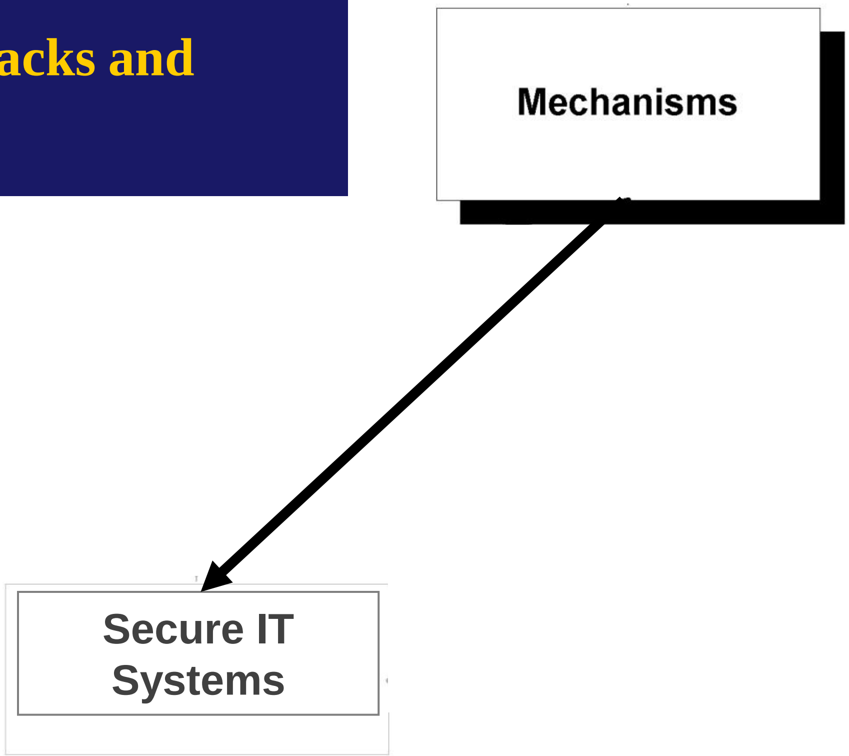
- Trend Micro



```
08/08/2014  05:04 PM    <DIR>          E-TNOSC
04/25/2014  06:54 PM    <DIR>          EMR Data
03/18/2014  11:10 AM    <DIR>          F-15 FMS
11/26/2014  12:56 PM    <DIR>          Gemini
10/17/2014  10:20 AM    <DIR>          Insitu
07/07/2014  11:47 AM    <DIR>          Integrated Catering & Camp Services
01/23/2014  05:47 PM    <DIR>          Iraq K9 Effort
11/06/2014  03:40 PM    <DIR>          ISAF-RS CJ7-TREX
09/02/2014  05:47 PM    <DIR>          Israel-USACE AEC MATOC
11/20/2014  01:56 PM    <DIR>          miscellaneous
10/23/2014  04:14 PM    <DIR>          MISTIF-A
06/03/2014  12:16 PM    <DIR>          NAVAIR PASS
05/18/2014  05:04 PM    <DIR>          NMEC EMS
02/17/2015  02:15 PM    <DIR>          OPSCEN
```

China's Operation Iron Tiger, Sept 2015

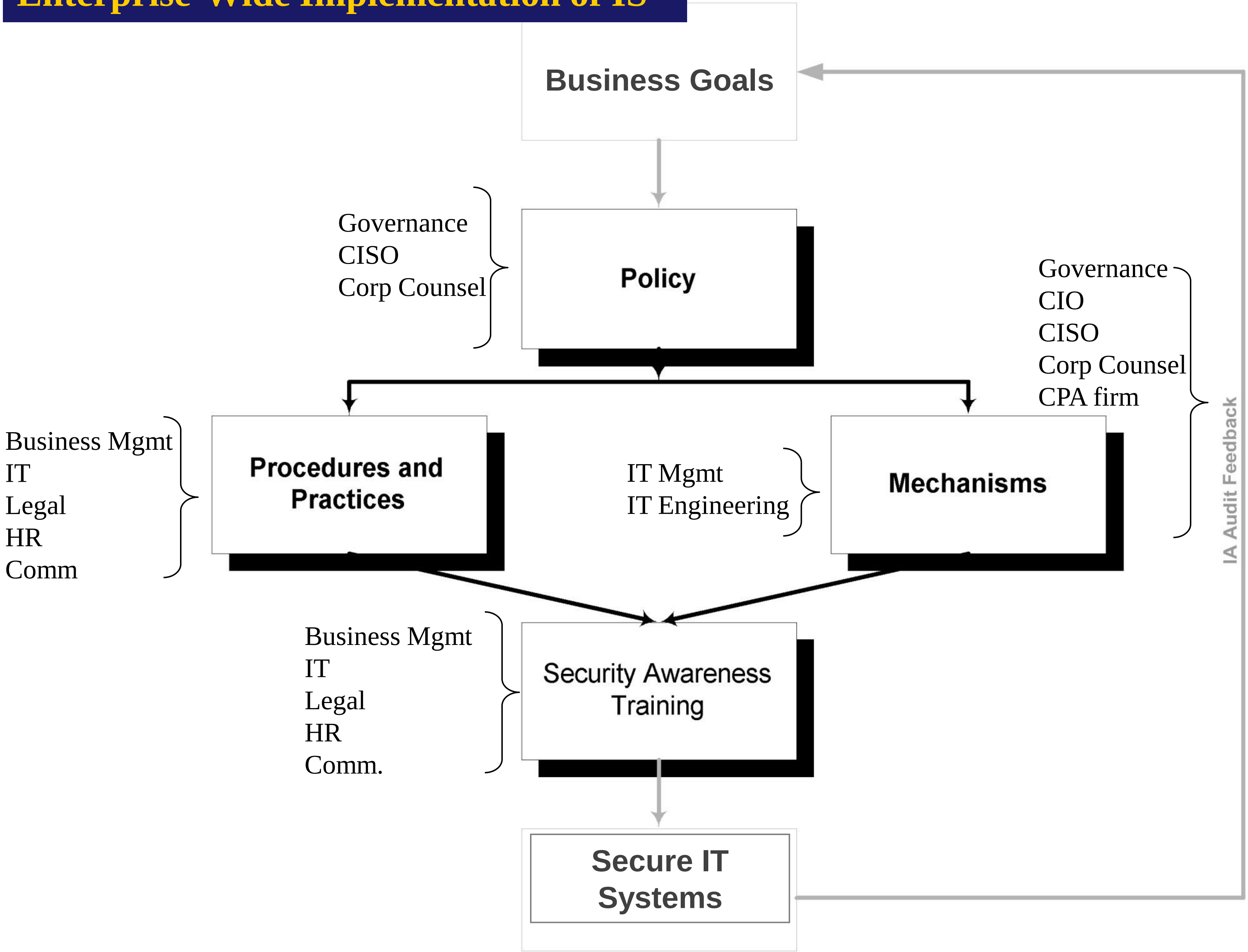
We learn Computer Security to countermeasure cyber attacks and protect IT systems!



Introduction

- The concept of computer security is evolving into the concept of Information Security
  - covers a broader range of issues from protection of data to protection of human resources
- Information security is the responsibility of every employee, especially managers

Enterprise-Wide Implementation of IS



Introduction

- Information security involves three distinct communities of interest
  - Information security managers and professionals
  - Information technology managers and professionals
  - Non-technical business managers and professionals

Communities of Interest

- **InfoSec community**
  - protects information assets from threats
- **IT community**
  - supports business objectives by supplying appropriate information technology
- **Business community**
  - articulates and communicates organizational policy and objectives
  - allocates resources to the other groups

What is Security?

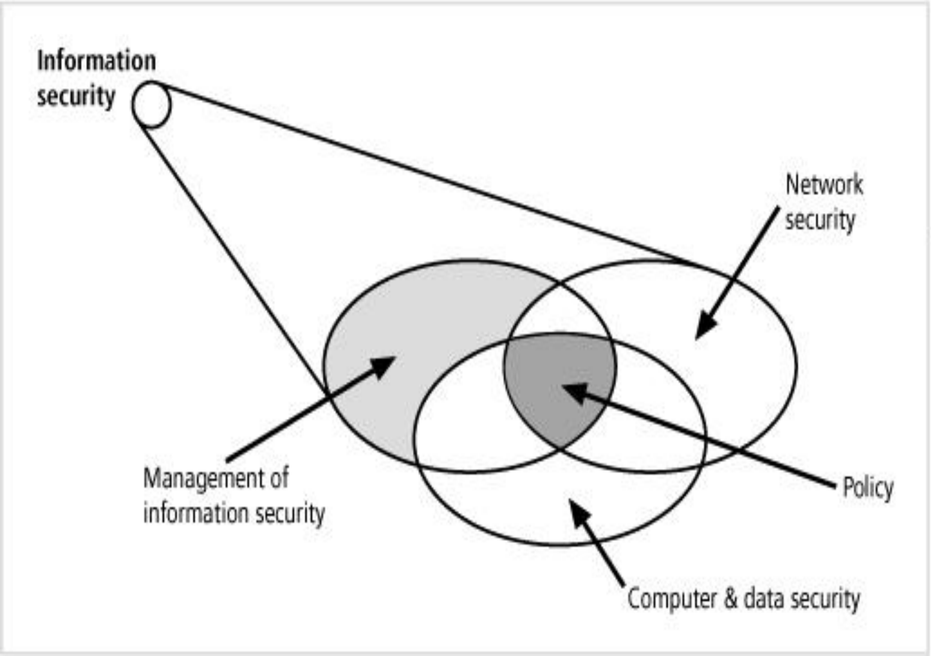
- **Security**: the quality or state of being secure – to be free from danger
  - to be protected from the risk of loss, damage, or unwanted modification, or other hazards
  - security is often achieved by means of several strategies undertaken simultaneously or used in combination with one another
  - management's role is to ensure that each strategy is properly planned, organized, staffed, directed, and controlled

What is Security?

- Specialized areas of security include:
  - **Physical security** - protecting people, physical assets, and the workplace from various threats
    - fire, unauthorized access, and natural disasters
  - **Operations security** - protecting the to carry out operational activities without interruption or compromise
  - **Communications security** - protecting communications media, technology, and content
  - **Network security** - protecting data networking devices, connections, and contents

What is Information Security?

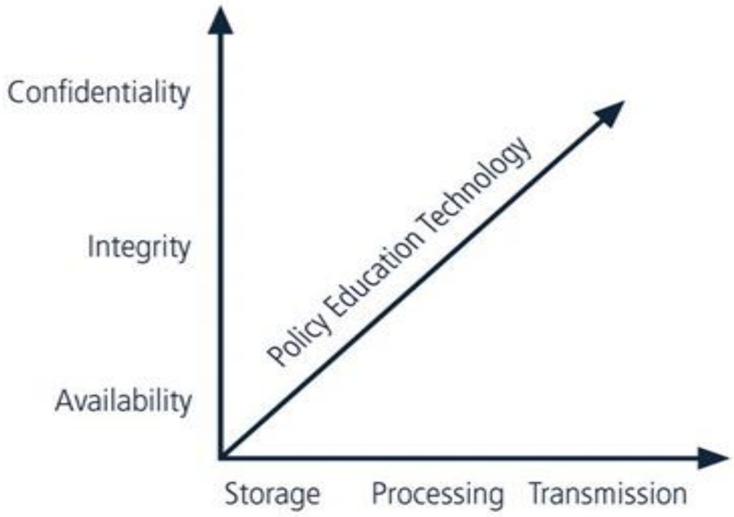
- **Information Security:** the protection of information and its critical elements (confidentiality, integrity and availability), including the systems and hardware that use, store, and transmit that information



Components of information security

CNSS Security Model

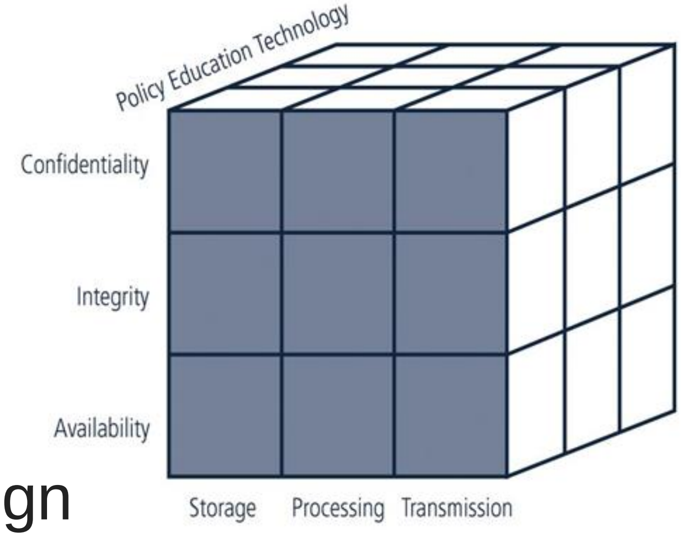
- NSTISSC (CNSS) Security Model (McCumber Cube)
  - serves as a standard for understanding aspects of InfoSec
  - main goal is to identify gaps in the coverage of an InfoSec program
- The model covers the three dimensions central to InfoSec:
  - information characteristics
  - information location
  - security control categories



CNSS Security Model

- Model is represented with a 3x3x3 cube of 27 cells
  - each cell represents an intersection among three dimensions
  - when using this model to design or review any InfoSec program, ensure each of the 27 cells is properly addressed
    - example: cell of "integrity x storage x technology"

"three layers deep"



CIA Triangle

- CNSS model is based on CIA
- **CIA triangle** is an industry standard for computer security since the development of the mainframe
  - confidentiality, integrity, availability
- Over time the list of characteristics has been expanded to include
  - *privacy*, *identification*, *authentication*, *authorization*, and *accountability*

Key Concepts of Information Security

- **Confidentiality**: only those with sufficient privileges and a demonstrated need may access it
  - Measures used to protect confidentiality:
    - Information classification
    - Secure document (and data) storage
    - Application of general security policies
    - Education of information custodians and end users
    - Cryptography (encryption)
  - Example:
    - Bell-LaPadula: no write up & no read down
    - TCSEC/TNI (DoD Orange, Red book)

Key Concepts of Information Security

- **Integrity:** the quality or state of being whole, complete, and uncorrupted
  - Information's integrity is threatened when exposed to corruption, damage, destruction, or other disruption of its authentic state
  - Error-control techniques: use of redundancy bits and check bits
  - Example: Biba (no write up & no read down), Clark-Wilson (separation of duty)

Key Concepts of Information Security

- **Availability**: authorized users have access to information in a usable format, without interference or obstruction
- **Privacy:** information is to be used
  - only for purposes known to the data owner
  - only in ways approved by the owner
  - Avoid privacy abuse: many organizations collect, swap, and sell personal information

Key Concepts of Information Security

- **Identification:** when an information system is able to recognize individual users
  - First step in gaining access to secured material
  - Serves as the foundation for subsequent authentication and authorization
  - Example: use of user name or ID

Key Concepts of Information Security

- **Authentication:** the process by which a control establishes whether a user (or system) has the identity it claims to have
  - Example: use of cryptographic certificates, secure token
- **Authorization:** a process that defines what an authenticated user has been specifically authorized by the proper authority to do
  - Example: access, modify, or delete information

Key Concepts of Information Security

- **Accountability:** occurs when a control provides assurance that every activity undertaken can be attributed to a named person or automated process
  - Example: audit logs

What is Management?

- To manage the information security process, first understand core principles of management
  - **Management** is the process of achieving objectives using a given set of resources
  - A **manager** is “someone who works with and through other people by coordinating their work activities in order to accomplish organizational goals”

Differences Between Leadership and Management

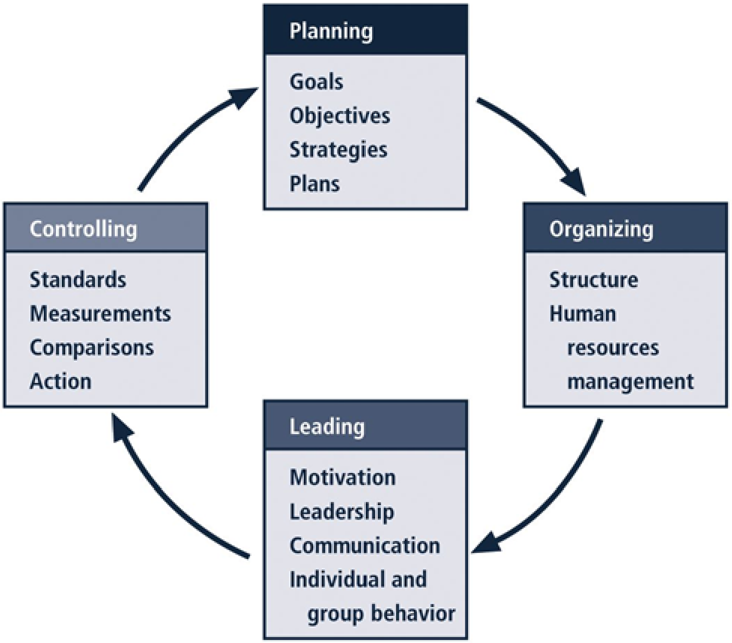
- The leader influences employees so that they are willing to accomplish objectives
  - leadership provides *purpose*, *direction*, and *motivation* to those that follow
  - *lead by example* and demonstrate personal traits that instill a desire in others to follow
- A manager administers the resources of the organization, budgets, authorizes expenditure

Managerial Roles

- **Decisional role** - selecting from among alternative approaches and resolving conflicts or challenges
- **Informational role** - collecting, processing, and using information to achieve objectives
- **Interpersonal role** - interacting with superiors, subordinates, outside stakeholders, and other parties that influence or are influenced by the completion of the task

Management Characteristics

- Two well-known management approaches:
  - *Popular management theory*
    - core principles of **p**lanning, **o**rganizing, **l**eading, and **c**ontrolling (POLC)
  - *Traditional management theory*
    - core principles of **p**lanning, **o**rganizing, **s**taffing, **d**irecting, and **c**ontrolling (POSDC)



Planning

- **Planning** - process of developing, creating, and implementing strategies to accomplish objectives
- Three levels of planning:
  - ***Strategic planning*** - highest levels of the organization, for a long period of time (~ >5 yr)
  - ***Tactical planning*** - integrates organizational resources at a level below the entire enterprise (~1-4 yr)
  - ***Operational planning*** - day-to-day operations, local resources, in the present or the short term

Organization

- **Organizing:** the structuring of resources to support the accomplishment of objectives
  - the structuring of departments and staff
  - the storage of raw materials to facilitate manufacturing
  - the collection of information

Leadership

- **Leading:** encouraging the implementation of the planning and organizing functions
  - Includes supervising employee behavior, performance, attendance, and attitude while ensuring completion of tasks, goals, and objectives
- Leadership generally addresses the direction and motivation of the human resource

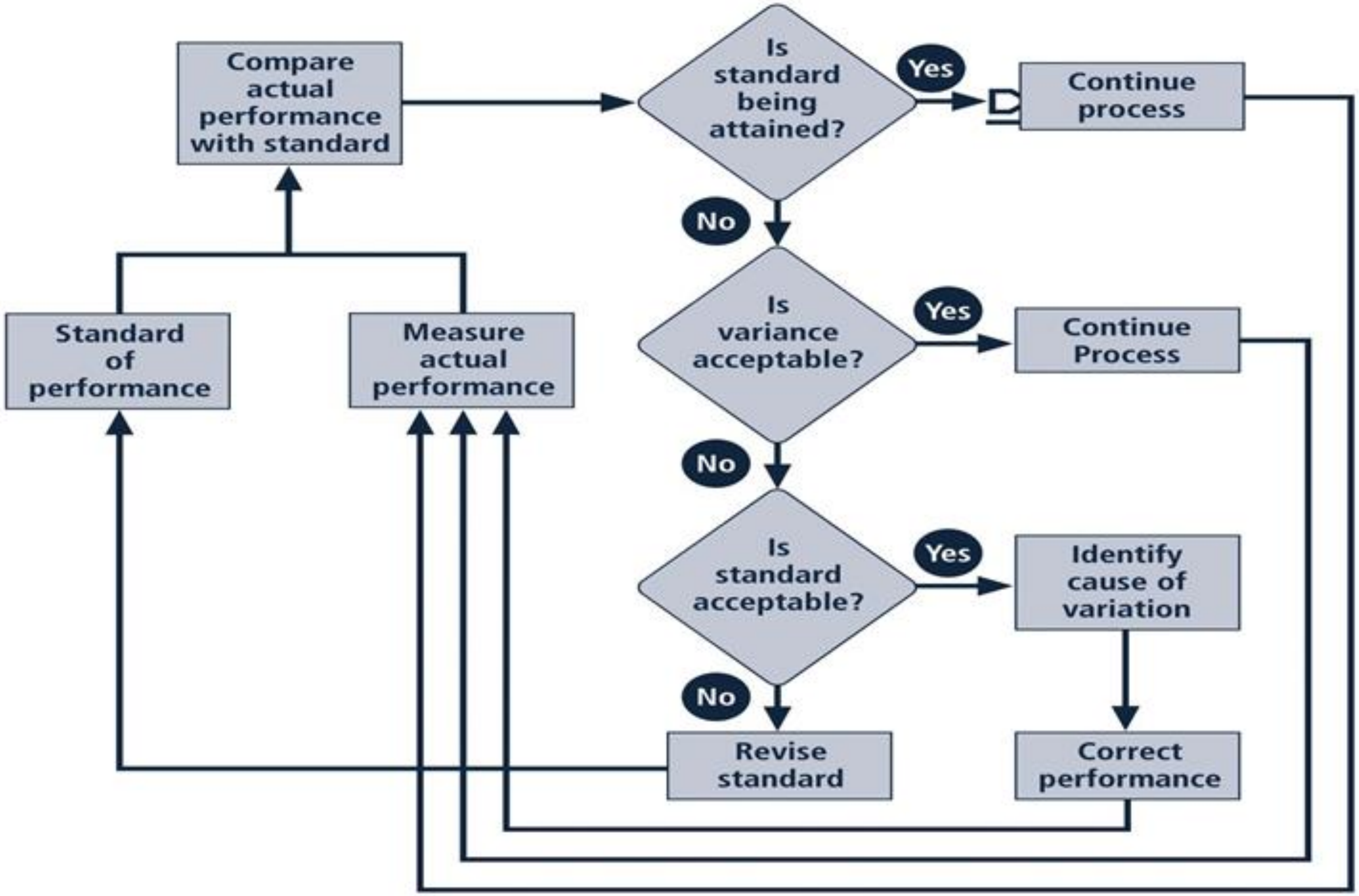
Control

- **Controlling:** ensures the validity of the organization’s plan
  - Monitoring progress toward completion
    - Sufficient progress is made
  - Making necessary adjustments to achieve desired objectives
    - Impediments to the completion of the task are resolved
    - No additional resources are required

Control Tools

- Controlling determines what must be monitored, and specific control tools to gather and evaluate information
- Four categories:
  - Information
    - Information flows/communications
  - Financial
    - Guide use of monetary resources (ROI, CBA,..)
  - Operational
    - PERT, Gantt, process flow
  - Behavioral
    - Human resources

The Control Process



Solving Problems

- Step 1: Recognize and define the problem
- Step 2: Gather facts and make assumptions
- Step 3: Develop possible solutions (Brainstorming)
- Step 4: Analyze and compare possible solutions (Feasibility analysis)
    - reviewing economic, technological, behavioral, and operational feasibilities
- Step 5: Select, implement, and evaluate a solution

Principles of Information Security Management

- The extended characteristics of information security are known as the **six P’s**
  - Planning
  - Policy
  - Programs
  - Protection
  - People
  - Project management

InfoSec Planning

- **Planning as part of InfoSec management**
  - is an extension of the basic planning model discussed earlier
- **Included in the InfoSec planning model are**
  - activities necessary to support the design, creation, and implementation of information security strategies as they exist within the IT planning environment

InfoSec Planning Types

- **Types of InfoSec plans:**
  - Incident response planning
  - Business continuity planning
  - Disaster recovery planning
  - Policy planning
  - Personnel planning
  - Technology rollout planning
  - Risk management planning
  - Security program planning

Policy

- Policy: set of organizational guidelines that dictates certain behavior within the organization
- In InfoSec, three general policy categories:
  - Enterprise information security policy (EISP)
    - sets the tone for the InfoSec department
  - Issue-specific security policy (ISSP)
    - sets of rules that define acceptable behavior within a specific technology, such as email, Internet use
  - System-specific policies (SysSPs)
    - controls the configuration and/or use of a piece of equipment or technology, such as ACLs

Programs

- Programs are operations that are specifically managed as separate entities
  - Example:
    - A security education training and awareness (SETA) program
  - Other types of programs
    - Physical security program
      - complete with fire protection, physical access, gates, guards, etc.
    - Programs dedicated to client/customer privacy and awareness

Protection

- Executed through a set of risk management activities including:
  - Risk assessment and control
  - Protection mechanisms
  - Technologies
  - Tools
- Each mechanism represents some aspect of the management of specific controls in the overall InfoSec plan

People

- People are the most critical link in the InfoSec program
  - Human firewall - educate workforce
- It is imperative that managers continuously recognize the crucial role that people play
- People in InfoSec includes
  - information security personnel
  - the security of personnel
  - the SETA program

Project Management

- Project management is to identify and control the resources applied to a project
- In InfoSec program, each process undertaken by the InfoSec group should be managed as a project
  - Example: implementing a new firewall