Management of Information Security, 4th Edition

Chapter 1

Introduction to the Management of Information Security

Objectives

- Describe the importance of the manager's role in securing an organization's use of technology
- List and discuss the key characteristics of information security
- Discuss the key characteristics of leadership and management
- Differentiate information security management from general business management
- Identify and describe basic project management practices and techniques

Introduction

- Information technology (IT)
  - Enables the storage and transportation of information from one business unit to another
  - IT systems can break down
- The concept of computer security has been replaced by the concept of information security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

Introduction (continued)

- Security funding and planning decisions should involve three distinct groups of decision makers, or **communities of interest**:
  - **Information security community** - protects the information assets of an organization
  - **Information technology community** - supports the business objectives by supplying and supporting IT that is appropriate to the organization's needs
  - **General business community** - articulates and communicates organizational policy and objectives and allocates resources to the other groups

What is Security? Part 1

- **Security**: the state of being secure—to be free from danger
- 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? Part 2

- 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 - 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 Security? Part 3

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

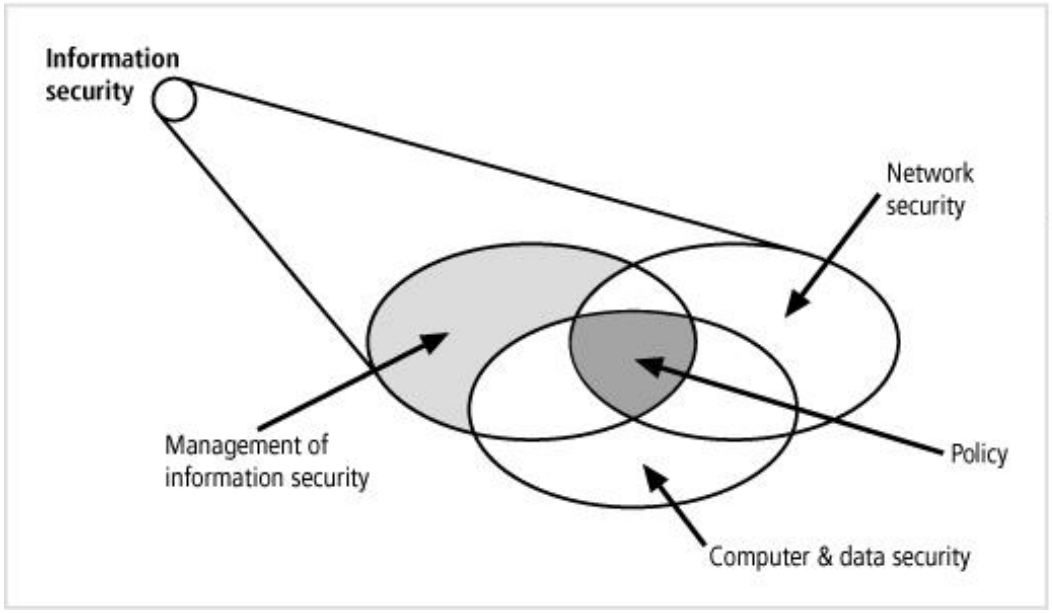
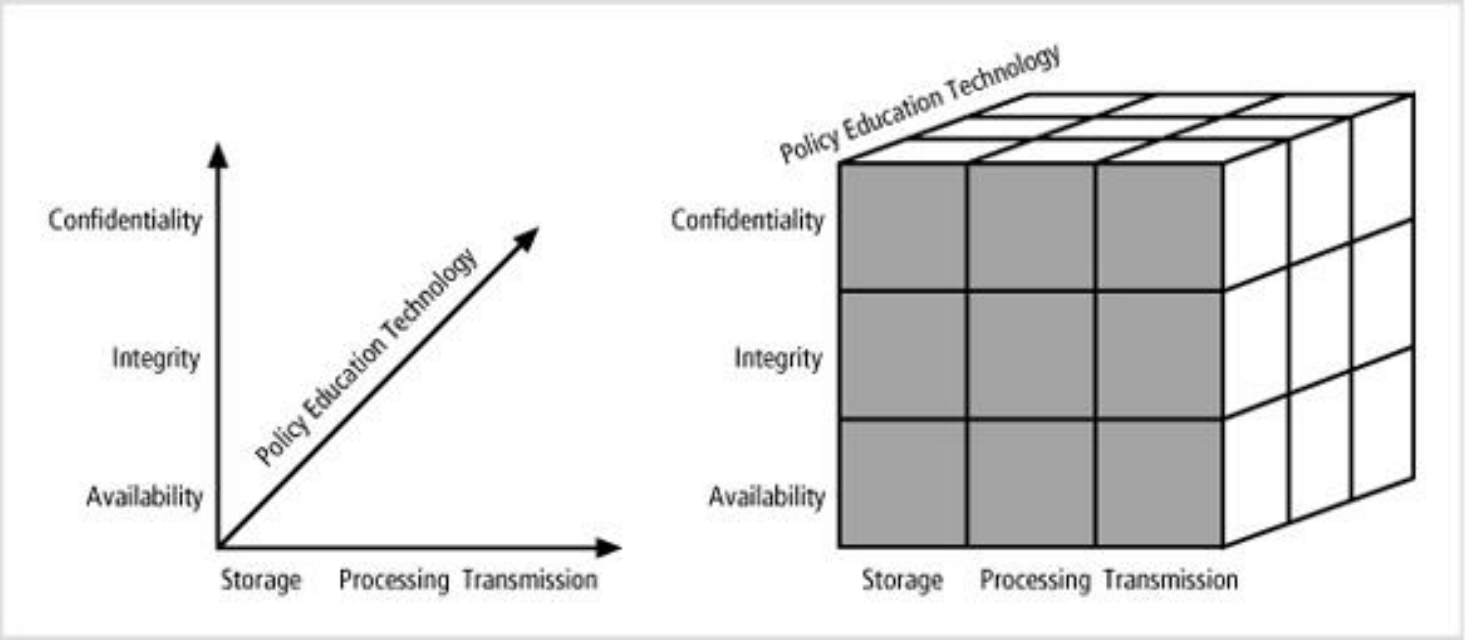


Figure 1-1 Components of information security

CNSS Security Model

- Committee on National Security Systems (CNSS) Also known as the McCumber Cube
  - Serves as the 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

Figure 1-2 CNSS security model



CNSS Security Model (continued)

- Model is represented with a 3x3x3 cube with 27 cells
  - Each cell represents an area of intersection among the three dimensions
- When using this model to design or review any InfoSec program:
  - Must make sure each of the 27 cells is properly addressing the use of technology to protect integrity of information while in storage

Key Concepts of Information Security Part 1

- C.I.A. triangle: industry standard for computer security since the development of the mainframe
  - Confidentiality, integrity, and availability are the characteristics of the original C.I.A triangle
- Due to today's constantly changing IT environment, the C.I.A. triangle has been expanded to include:
  - Privacy, identification, authentication, authorization, and accountability

Key Concepts of Information Security Part 2

- **Confidentiality**: only those with sufficient privileges and a demonstrated need may access it
- Measures used to protect the confidentiality of information:
  - Information classification
  - Secure document (and data) storage
  - Application of general security policies
  - Education of information custodians and end users
  - Cryptography (encryption)
- Closely related to privacy

Key Concepts of Information Security Part 3

- **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
- **Availability**: authorized users have access to information in a usable format, without interference or obstruction

Key Concepts of Information Security Part 4

- **Privacy:** information will be used only in ways approved by the person who provided it
  - Many organizations collect, swap, and sell personal information
- **Identification:** when an information system is able to recognize individual users
  - First step in gaining access to secured material and serves as the foundation for subsequent authentication and authorization
  - Typically performed by means of a user name or ID

Key Concepts of Information Security Part 5

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

What is Management?

- **Management:** the process of achieving objectives using a given set of resources
- Roles of management:
  - **Informational role** - collecting, processing, and using information that can affect the completion of the objective
  - **Interpersonal role** - interacting with superiors, subordinates, outside stakeholders, and other parties that influence or are influenced by the completion of the task
  - **Decisional role** - selecting from among alternative approaches and resolving conflicts or challenges

Management Characteristics Part 1

- Two basic approaches to management:
  - *Traditional management theory* - uses the core principles of planning, organizing, staffing, directing, and controlling (POSDC)
  - *Popular management theory* - uses the core principles of planning, organizing, leading, and controlling (POLC)
- The traditional management theory is often well covered in business courses
  - Here we will focus on the POLC principles

Management Characteristics Part 2

- **Planning** - process of developing, creating, and implementing strategies to accomplish objectives
- Three levels of planning:
  - *Strategic planning* - occurs at the highest levels of the organization and for a long period of time
  - *Tactical planning* - focuses on production planning and integrates organizational resources at a level below the entire enterprise
  - *Operational planning* - focuses on the day-to-day operations of local resources and occurs in the present or the short term

Management Characteristics Part 3

- Planning begins with the creation of strategic plans for the entire organization
  - Resulting plan is divided into planning elements relevant to each major business unit of the organization
  - Business units create business plans that meet the requirements of the overall organizational strategy
  - Plans are communicated to mid-level managers and supervisors to create operational plans
- **Objective**: an intermediate point that allows you to measure progress toward the goal

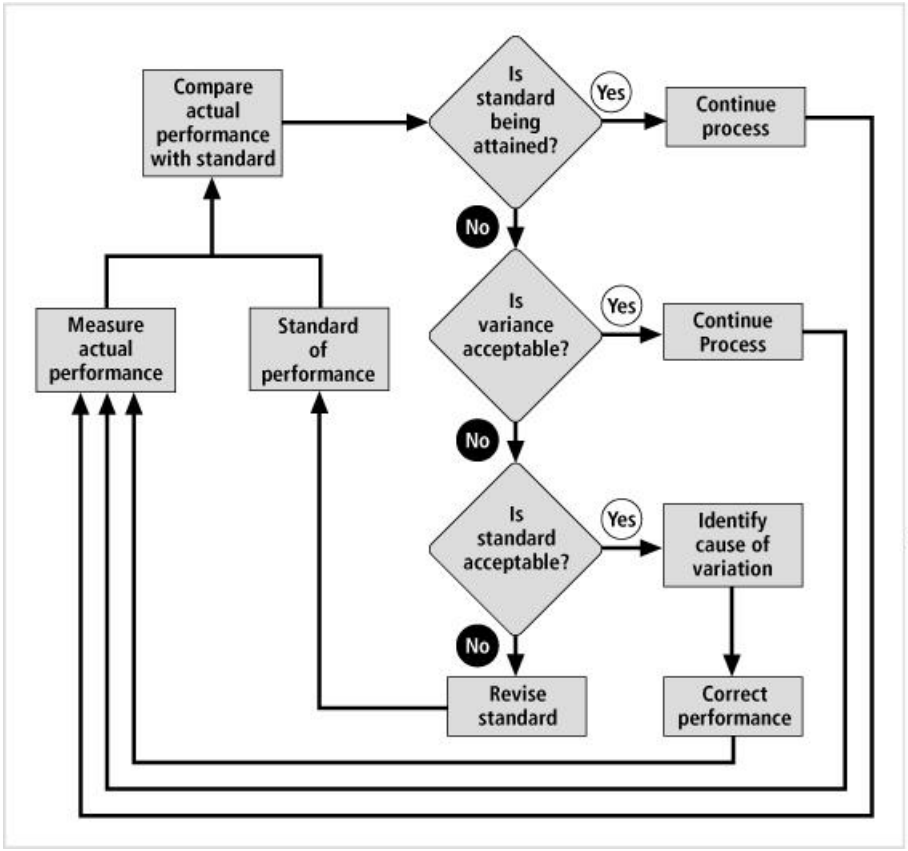
Management Characteristics Part 4

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

Management Characteristics Part 5

- **Controlling:** monitoring progress toward completion and making necessary adjustments to achieve desired objectives
  - Ensures the validity of the organization's plan
- The manager ensures that:
  - Sufficient progress is made
  - Impediments to the completion of the task are resolved
  - No additional resources are required

Figure 1-4 The control process



Solving Problems

- Step 1: Recognize and define the problem
- Step 2: Gather facts and make assumptions
- Step 3: Develop possible solutions
- Step 4: Analyze and compare possible solutions
  - Analysis may include 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
  - Projects

Planning

- The planning model includes activities necessary to support the design, creation, and implementation of InfoSec strategies
- Types of InfoSec plans:
  - Incident response planning
  - Business continuity planning
  - Disaster recovery planning
  - Policy planning and Personnel planning
  - Technology rollout planning
  - Risk management planning and Security program planning

Policy

- Policy: the set of organizational guidelines that dictates certain behavior within the organization
- Three general policy categories:
  - *Enterprise information security policy (EISP)*
  - *Issue-specific security policy (ISSP)*
  - *System-specific policies (SysSPs)*

Policy…

- 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
  - *System-specific policies (SysSPs)* - control the configuration and/or use of a piece of equipment or technology

Programs

- **Programs**: InfoSec 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 client/customer privacy and awareness

Protection

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

People and Projects

- People are the most critical link in the InfoSec program
  - Encompasses security personnel
- Each process undertaken by the InfoSec group should be managed as a project
  - Example: implementing a new firewall

Project Management Part 1

- Project management involves:
  - Identifying and controlling the resources applied to the project
  - Measuring progress
  - Adjusting the process as progress is made
- Projects are discrete sequences of activities with starting points and defined completion points

Project Management Part 2

- Project management involves the temporary assembling of a group to complete the project
  - After completion, its members are released and perhaps assigned to other projects
- Some projects are iterative and occur regularly
  - Example: budgeting processes
- Another common practice is the creation of a sequence of projects
  - With periodic submission of grouped deliverables

Project Management Part 3

- Benefits of project management skills:
  - Implementing a methodology ensures that no steps are missed
  - Creating a blueprint of project activities serves as a common reference tool and improves productivity
  - Identifying specific responsibilities for all the involved personnel reduces ambiguity
  - Clearly defining project constraints and minimum quality requirements increases the likelihood that the project will stay within them

Project Management Part 4

- Benefits of project management skills (cont'd):
  - Establishing performance measures and creating project milestones simplifies project monitoring
  - Identifying deviations in quality, time, or budget early on enables early correction of the problems
- **A project is considered a success when:**
  - It is completed on time or early
  - It is completed at or below its budgeted amount
  - It meets all specifications outlined in the approved project definition, and all deliverables are accepted by the end user

Applying Project Management to Security

- To apply project management to InfoSec, you must select an established project management methodology
- InfoSec project managers often follow methodologies based on the PMBoK
  - PMBoK is considered the industry best practice
  - Other project management approaches do exist

PMBoK Knowledge Areas Part 1

- **Project Integration Management** includes:
  - Processes required to ensure effective coordination occurs within and between the project's components
- Major elements of project management that require integration include:
  - Development of the initial project plan
  - Monitoring of progress as the project plan is executed
  - Control of the revisions to the project plan as well as control of the changes made to resource allocations

PMBoK Knowledge Areas Part 2

- Conflicts among Communities of Interest
  - When IT staff are not completely aligned with the objectives of the InfoSec project, they may make less of an effort toward ensuring its success
  - Must educate and inform other communities of interest
- Resistance to New Technology
  - InfoSec projects often introduce new technologies
  - Project team members, as well as other workers, may require special training when new technologies are introduced

PMBoK Knowledge Areas Part 3

- **Project Scope Management** - ensures that the project plan includes only those activities that are necessary to complete it
- One thing that undermines many projects once they are underway is **scope creep**
  - Occurs when the quantity or quality of project deliverables is expanded from the original plan
  - Stopping it may include asking for an expansion of work time or project resources
- Scope management includes scope planning, scope definition, and scope verification

PMBoK Knowledge Areas Part 4

- **Project Time Management** - ensures that the project is finished by the identified completion date while meeting its objectives
  - Failure to meet deadlines is one of the most frequent failures in project management
- Project time management includes these processes:
  - Activity definition, activity sequencing, activity duration estimating, schedule development, schedule control

PMBoK Knowledge Areas Part 5

- **Project Cost Management** - processes required to ensure a project is completed within the resource constraints placed on it
- Project cost management includes these processes:
  - Resource planning
  - Cost estimating
  - Cost budgeting
  - Cost control

PMBoK Knowledge Areas Part 6

- **Project Quality Management** - processes required to ensure that the project adequately meets the project specifications
- A good project plan defines project deliverables in unambiguous terms against which actual results are easily compared
- Project quality management includes:
  - Quality planning, quality assurance, and quality control

PMBoK Knowledge Areas Part 7

- **Project Human Resource Management** - ensures that the personnel assigned to a project are effectively employed
- Staffing a project requires careful estimates:
  - Too few people may mean it will not be completed on time
  - Too many working on a project may be an inefficient use of resources
- Project human resource management includes organizational planning, staff acquisition, and team development

PMBoK Knowledge Areas Part 8

- Management of human resources must address:
  - Not all workers operate at the same level of efficiency
  - Not all workers begin the project assignment with the same degree of skill
  - Skill mixtures among actual project workers seldom match the needs of the project plan
  - Some tasks may require skills that are not available from resources on hand

PMBoK Knowledge Areas Part 9

- **Project Communications Management** - processes necessary to convey to all involved parties the details of activities associated with the project
- Project communication management includes:
  - Communication planning, information distribution, performance reporting, and administrative closure

PMBoK Knowledge Areas Part 10

- **Project Risk Management** - processes necessary to assess, mitigate, manage, and reduce the impact of adverse occurrences on the project
- Project risk management includes:
  - Risk identification
  - Risk quantification
  - Risk response development
  - Risk response control

PMBoK Knowledge Areas Part 11

- **Project Procurement Management** - processes necessary to acquire needed resources to complete the project
- InfoSec projects may have more complex needs
  - More likely to need special software or hardware products and/or skilled human resources

Project Management Tools

- Most project managers use tools to facilitate scheduling and execution of the project
- **Projectitis**: occurs when the project manager spends more time documenting project tasks, collecting performance measurements, recording project task information, and updating project completion forecasts than accomplishing meaningful project work

Work Breakdown Structure

- **Work breakdown structure (WBS):** a planning tool that can be used with a spreadsheet program as wells with a project management software tool
- The project plan is broken down into major tasks

Table 1-2 Example of an early-draft work breakdown structure

Task	Effort (hours)	Skill	Dependencies
1. Contact field office and confirm network assumptions	2	Network architect	
2. Purchase standard firewall hardware	4	Network architect and purchasing group	1
3. Configure firewall	8	Network architect	2
4. Package and ship firewall to field office	2	Intern	3
5. Work with local technical resource to install and test firewall	6	Network architect	4
6. Complete network vulnerability assessment	12	Network architect and penetration test team	5
7. Get remote office sign-off and update network drawings and documentation	8	Network architect	6

Task-Sequencing Approaches Part 1

- Several approaches are available to assist the project manager in the sequencing effort
- **Network scheduling**: a task-sequencing method
  - Example: Activity A must occur before activity B, which must occur before activity C

Figures 1-7 and 1-8, Examples of Simple and Complex Dependency

Figure 1-7 Example of a simple network dependency

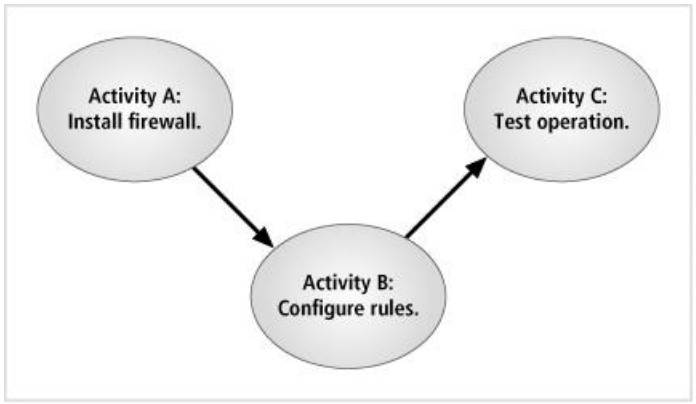
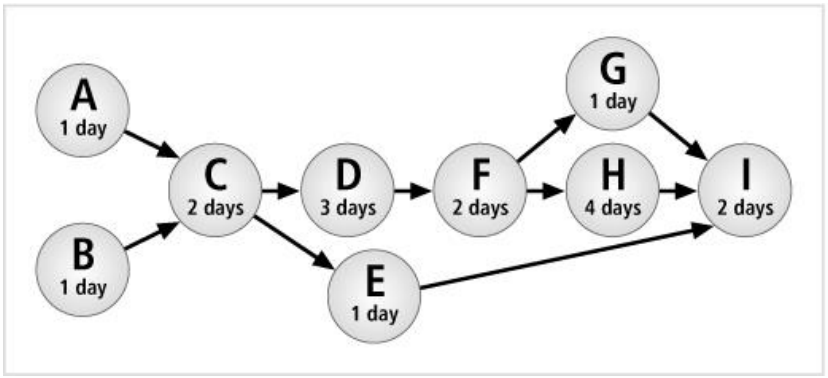


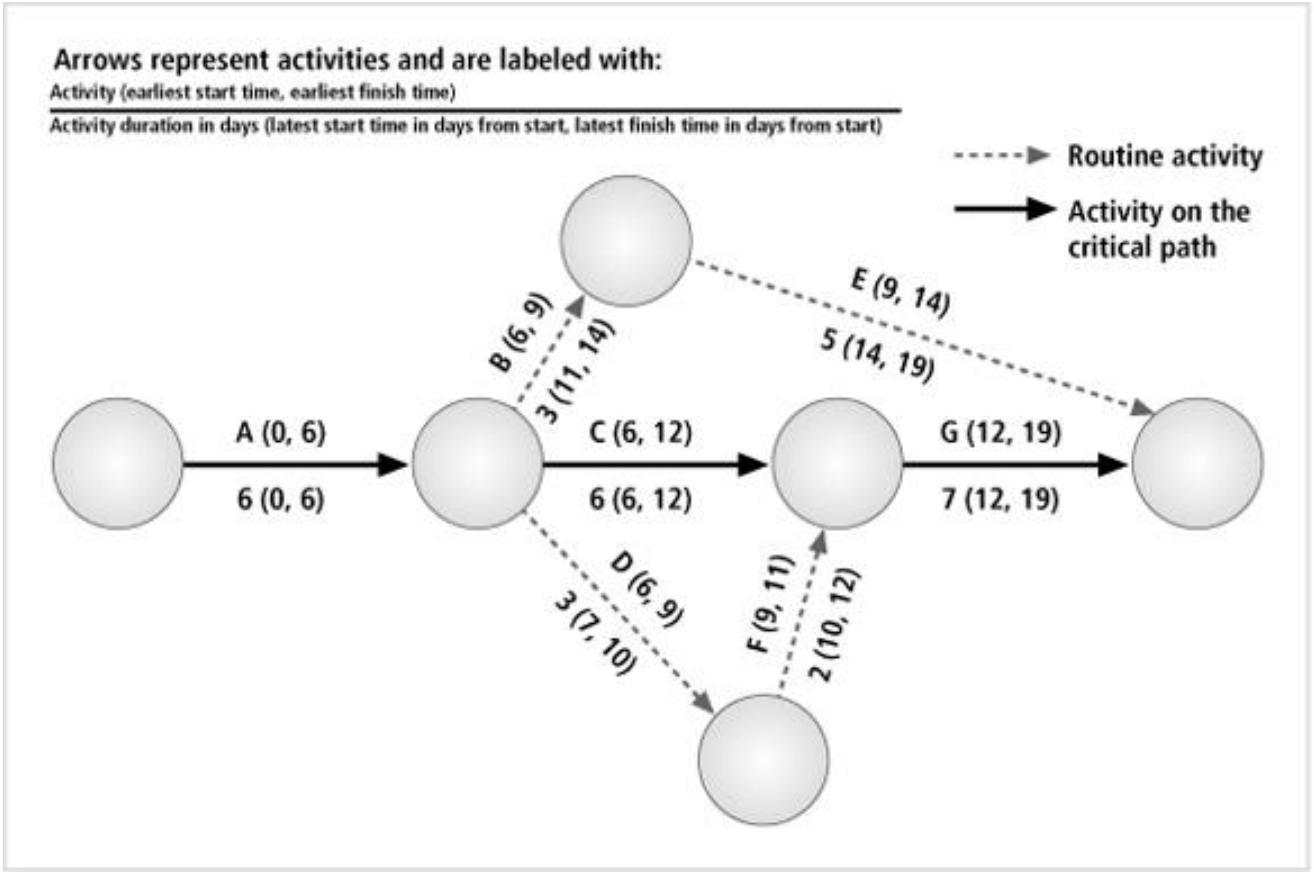
Figure 1-8 Example of a complex network dependency



Task-Sequencing Approaches Part 2

- **Program Evaluation and Review Technique (PERT):** most popular networking dependency diagramming technique
- IT is possible to diagram a complex operation if you can answer three key questions:
  - How long will the activity take?
  - What activity occurs before this activity can take place?
  - What activity occurs after this activity?

Figure 1-9 Example of a PERT



Task-Sequencing Approaches Part 3

- PERT (cont'd)
  - By identifying the path through various activities, you can determine the **critical path**
  - **Slack time**: difference in time between the critical path and any other path

Task-Sequencing Approaches Part 4

- Advantages of using the PERT method:
  - Planning large projects is made easier by facilitating the identification of pre- and post-activities
  - Planning to determine the probability of meeting requirements is allowed
  - The impact of changes on the system is anticipated
  - Information is presented in a straightforward format that both technical and nontechnical managers can understand and refer to in planning discussions
  - No formal training is required

Task-Sequencing Approaches Part 5

- Disadvantages of using the PERT method:
  - Diagrams can become awkward and cumbersome
  - Diagrams can become expensive to develop and maintain
  - It can be difficult to place an accurate “time to complete” on some tasks
- **Critical Path Method(CPM):** a method similar to PERT designed to identify the sequence of tasks that make up the shortest elapsed time to complete the project

Task-Sequencing Approaches Part 6

- Gantt Chart: a popular project management tool
  - Simple to read and understand
  - Uses bar charts

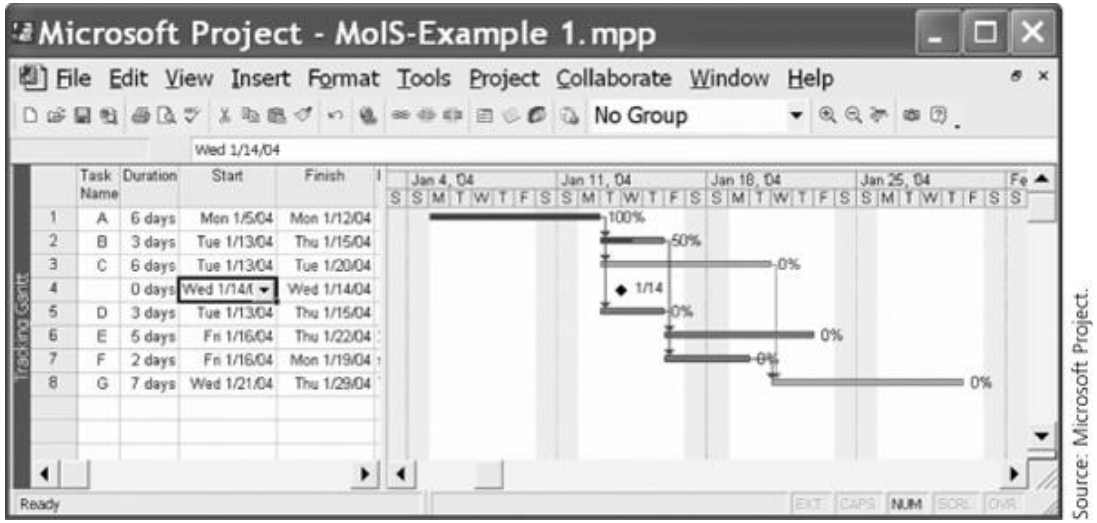


Figure 1-10 Example of a Gantt chart

Automated Project Tools

- Microsoft Project: considered to be the most widely used project management tool
- If you are considering using an automated project management tool, keep the following in mind:
  - A software program cannot take the place of a skilled and experienced project manager
  - A software tool can get in the way of work
  - Choose a tool that you can use effectively

Summary Part 1

- The concept of computer security has been replaced by the concept of InfoSec
- Organizations often have three communities of interest: InfoSec managers and professionals, IT managers and professionals, and nontechnical managers and professionals
- In its simplest form, management is the process of achieving objectives by using resources
- The traditional approach to management theory uses the core principles of planning, organizing, staffing, directing, and controlling (POSDC)

Summary Part 2

- The process that develops, creates, and implements strategies for the accomplishment of objectives is called “planning”
- InfoSec management operates like all other management units, but the goals and objectives of the InfoSec management team are different in that they focus on the secure operation of the organization
- Project management is the application of knowledge, skills, tools, and techniques to project activities to meet project requirements

Summary Part 3

- The creation of a project plan can be accomplished using a very simple planning tool, such as the work breakdown structure (WBS)
- A set of methods that can be used to sequence the tasks and subtasks in a project plan is known as “network scheduling”
- Automated project management tools can assist experienced project managers in the complexities of managing a large project but may get in the way when used on simple projects