INTRODUCTION TO NETWORK SECURITY PROJECT MANAGEMENT

LECTURE 1

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DR. ZAHEERA BINTI ZAINAL ABIDIN

CONTENT

- INTRODUCTION
  - OVERVIEW
    - Idea of Network Security and Project Management
    - Definition of Network Security Project Management
  - CONCEPT OF CORPORATE IT
  - COMPONENT OF NETWORK SECURITY PROJECT MANAGEMENT
  - NETWORK SECURITY PLANNING MANAGEMENT PLAN

LEARNING OUTCOMES

- Students should be able to:
  - Identify the processes, tools and techniques in network security project management.
  - Demonstrate the understanding of all project management body of knowledge (i.e. processes, tools and techniques).
  - Organize projects which related to Information Technology and Network Security.

LEARNING OBJECTIVES – 1

Upon completion of this chapter, you should be able to:

- Explain the meaning of project, provide examples of information technology projects, list various attributes of projects, and describe the triple constraint of projects.
- Describe project management and discuss key elements of the project management framework, including project stakeholders, the project management knowledge areas, common tools and techniques, and project success.
- Understand the growing need for better project management, especially for information technology projects.

LEARNING OBJECTIVES – 2

- Understand the role of the project manager by describing what project managers do, what skills they need, and what the career field is like for information technology project managers.
- Discuss the relationship between project, program, and portfolio management and the contributions they each make to enterprise success.
- Evaluate available network security project management tools.

INTRODUCTION

OVERVIEW (i.e.: TERMINOLOGY, DEFINITION AND SCOPE)

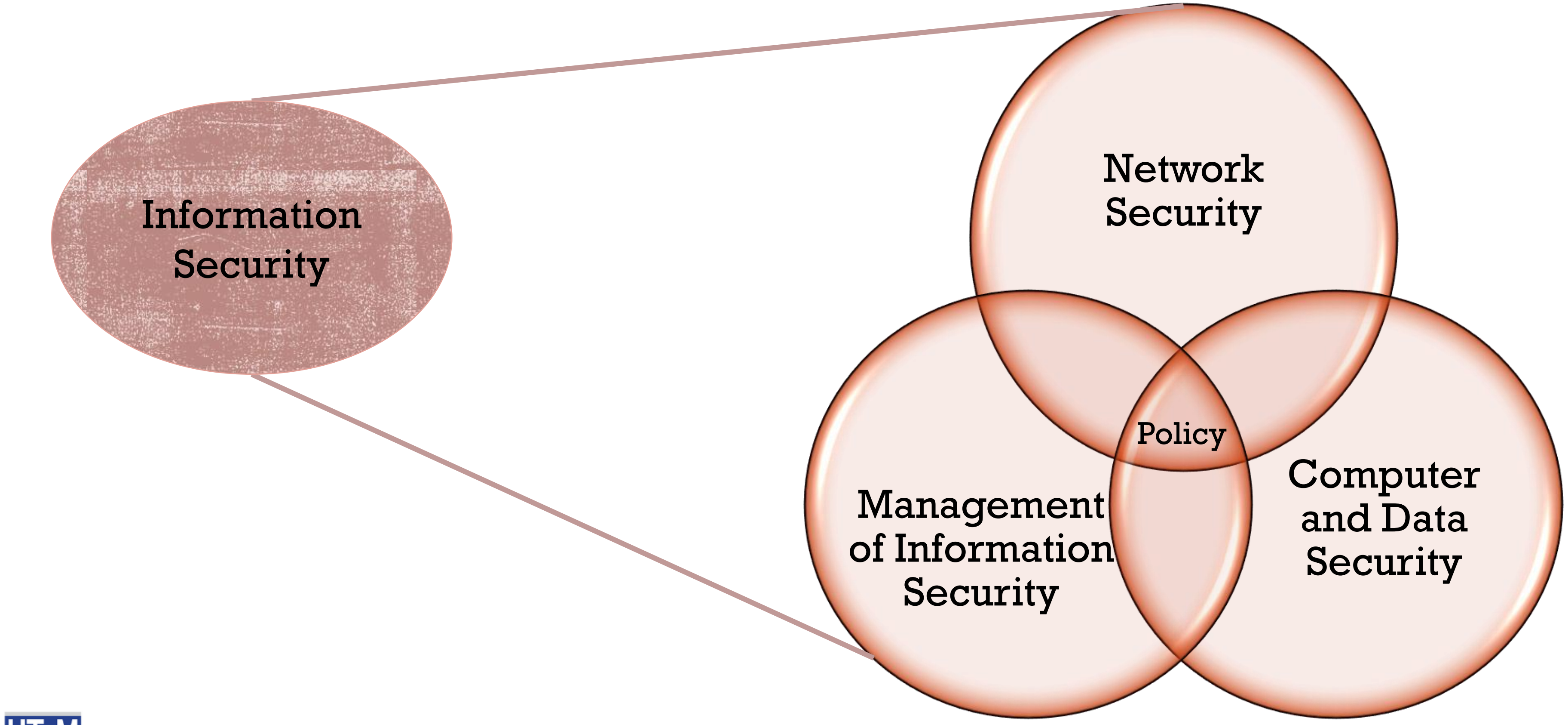
CONCEPTS OF CORPORATE AND IT ORGANIZATION

NETWORK SECURITY PROJECT MANAGEMENT PLAN DESCRIPTION

OVERVIEW

- IDEA, TERMINOLOGY AND DEFINITION

IDEA OF NETWORK SECURITY PROJECT MANAGEMENT



Information Security

Network Security

Policy

Management of Information Security

Computer and Data Security

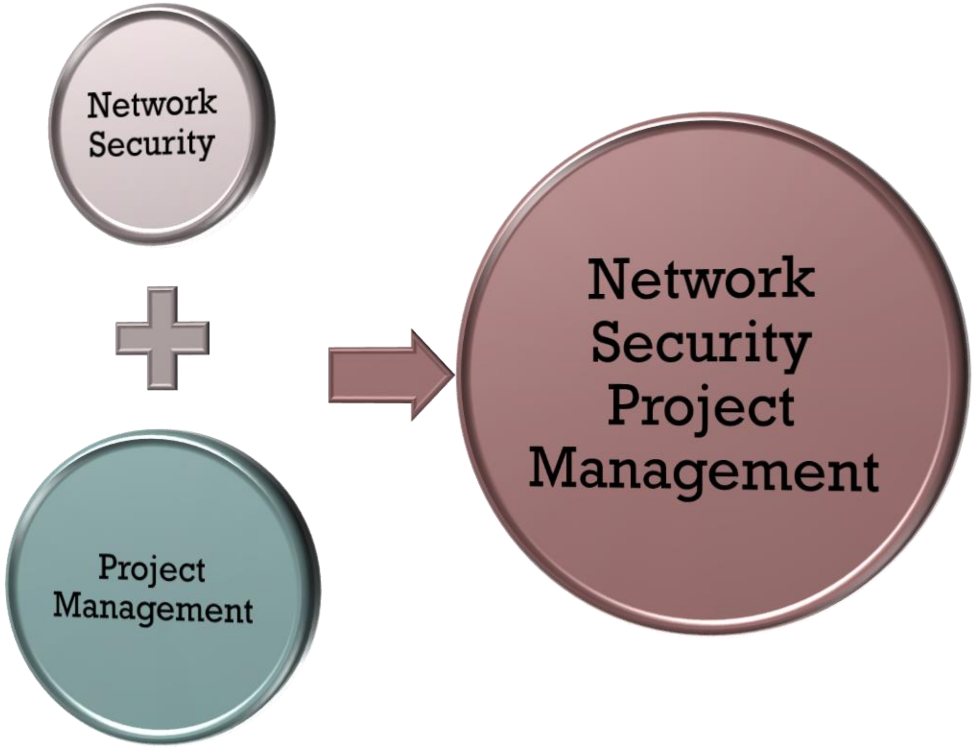
IDEA OF NETWORK SECURITY PROJECT MANAGEMENT

- An integration of project management into securing the network helps network engineers to manage the project well.
- The main purpose of network security project management is to provide data security and a safe network environment using a systematic approach.

IDEA OF NETWORK SECURITY PROJECT MANAGEMENT

- Technical experts without the managerial and good communication skills produce a FAILURE to the project implementation.

- To make a project SUCCESS, project manager needs a good leadership, ethics, management skills and entrepreneur skills instead of the technical skills.



OVERVIEW – 1

- The Internet brings millions of computer networks to communicate with each other—many of them unsecured.

- Ability to secure a computer's data influenced by the security of every computer to which it is connected.

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

OVERVIEW – 2 : CASE STUDIES

- A PricewaterhouseCoopers study found that overall, half of all projects fail and only 2.5% of corporations consistently meet their targets for scope, time, and cost goals for all types of project.
- A 1995 Standish Group study (CHAOS) found that only 16.2% of IT projects were successful in meeting scope, time, and cost goals; over 31% of IT projects were canceled before completion.
- In Computerworld Magazine (2008) stated that more than 35% IT companies project failures and off track with over budget.

THE NEED TO INTEGRATE SECURITY IN NETWORK PROJECTS

- Balance between cost and security controls need to be achieved
- Management consideration is required for defining security needs (based on risk analysis)

BENEFITS OF NETWORK SECURITY PROJECT MANAGEMENT

- Better control of financial, physical and personnel.
- Improved customer relations.
- Shorter development times.
- Low costs.
- Increase quality.
- Increase profit margin.
- Increase security.

DEFINITION OF PROJECT ?

- A **project** is "a temporary endeavor undertaken to create a unique product, service, or result" (PMBOK® Guide, Fourth Edition, 2008, p. 5).
- Operations is work done to sustain the business.
- Projects end when their objectives have been reached or the project has been terminated.
- Projects can be large or small and take a short or long time to complete.

DEFINITION OF PROJECT MANAGEMENT ?

- **Project management** is "the application of knowledge, skills, tools and techniques to project activities to meet project requirements" (PMBOK® Guide, Fourth Edition, 2008, p. 6).

- Project managers strive to meet the **triple constraint** by balancing project scope, time, and cost goals. However, in order to create a dynamic and behavioral environment to network project, the **quartet constraint** is introduced by inserting the element of people.

- Project management is a methodical approach to planning and guiding project processes from start to finish. According to the Project Management Institute, the processes are guided through five (5) stages: initiation, planning, executing, controlling, and closing. Project management can be applied to almost any type of project and is widely used to control the complex processes of software development projects.

DEFINITION OF NETWORK SECURITY

- Network security consists of policies adopted to prevent and monitor authorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.
- Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals, which involved in organizations, enterprises, and other types of institutions. It secures the network, as well as protecting and overseeing operations being done.

TERMINOLOGY OF NETWORK SECURITY PROJECT MANAGEMENT

- **Network Security Project Management (NSPM) is the measure to secure the network against internal or external attacks either in real or cyber world using quality assurance and risk analysis based on quartet constraints (scope, cost, time and people).**

CONCEPTS OF CORPORATE AND INFORMATION TECHNOLOGY ORGANIZATION

- Definition
- Components
- Security Constraints and Planning
- Impact of Security in IT Company

CORPORATE & IT ORGANIZATION

- In previous time, IT is treated as a unit or department in an organization, However as business is growing and the demand for a better management in IT unit has evolved proportional with the need. Thus, IT unit has been upgraded to be called as Corporate IT.
- **Corporation** is a business or **organization** formed by a group of people, and it has rights and liabilities to separate from those of the individuals involved.
- It may be a nonprofit organization engaged in activities for the public good; a municipal corporation, such as a city or town; or a private corporation which has been organized to make a profit.
- A **corporate structure** consists of various departments that contribute to the organization's mission and goals. Common major departments include Marketing, Finance, Accounting, Human Resource, and IT.
- Corporate IT is the department within an organization charged with establishing, monitoring and maintaining information technology systems and services, and with strategic planning around current and future IT initiatives.

10 CRITERIA OF ORGANIZATIONAL CULTURE

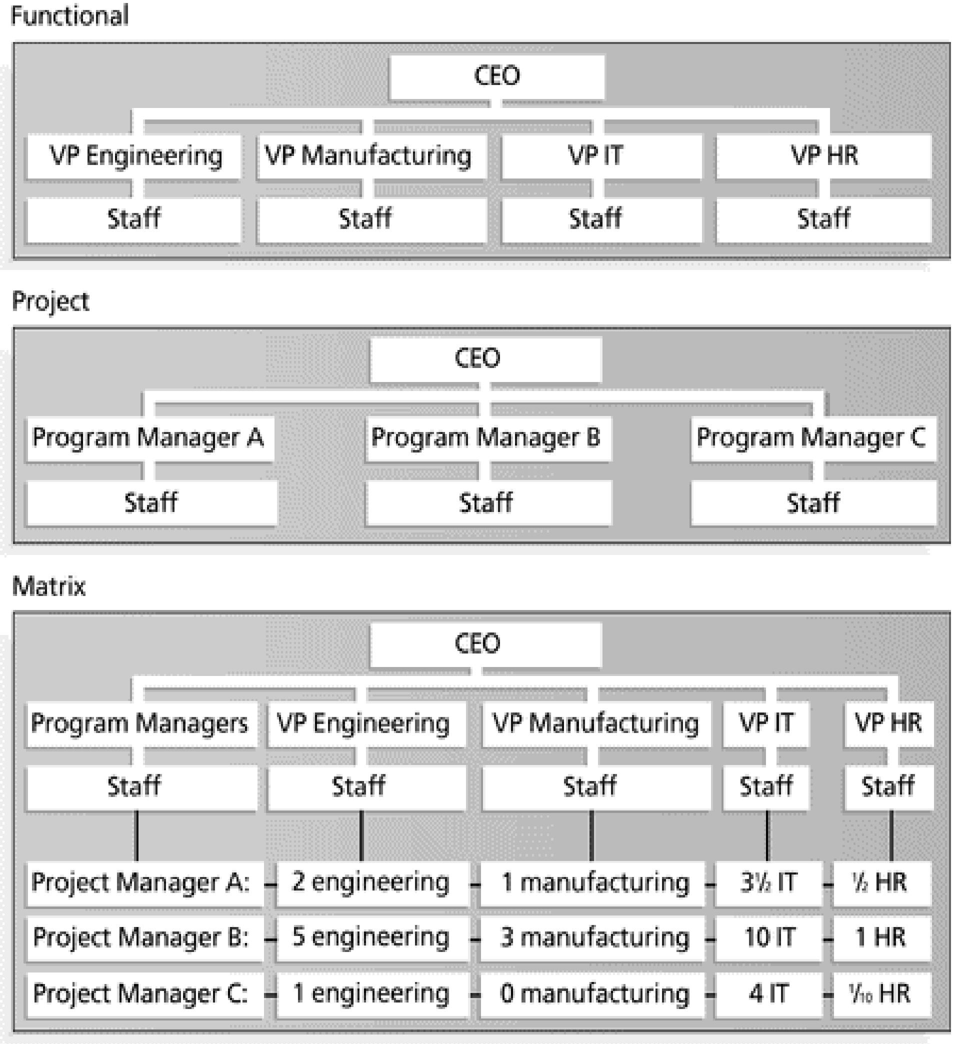
- Member Identity
- People Focus
- Unit Integration
- Control
- Group Emphasis

- Risk Tolerance
- Reward Criteria
- Conflict Tolerance
- Open-Systems Focus
- Means-ends orientation

ORGANIZATIONAL STRUCTURES

- 3 basic organization structures
  - **Functional**: functional managers report to the CEO
  - **Project**: program managers report to the CEO
  - **Matrix**: middle ground between functional and project structures; personnel often report to two or more bosses; structure can be weak, balanced, or strong matrix

FUNCTIONAL, PROJECT, AND MATRIX ORGANIZATIONAL STRUCTURES



Functional

CEO

VP Engineering — Staff

VP Manufacturing — Staff

VP IT — Staff

VP HR — Staff

Project

CEO

Program Manager A — Staff

Program Manager B — Staff

Program Manager C — Staff

Matrix

CEO

Program Managers — Staff

VP Engineering — Staff

VP Manufacturing — Staff

VP IT — Staff

VP HR — Staff

Project Manager A:	2 engineering	1 manufacturing	3½ IT	½ HR
Project Manager B:	5 engineering	3 manufacturing	10 IT	1 HR
Project Manager C:	1 engineering	0 manufacturing	4 IT	⅒ HR

ORGANIZATIONAL STRUCTURE INFLUENCES ON PROJECTS

Project Characteristics	**Organizational Structure Type**				
	Functional	**Matrix**			**Project**
		Weak Matrix	***Balanced Matrix***	***Strong Matrix***	
Project manager’s authority	Little or none	Limited	Low to Moderate	Moderate to high	High to almost total
Percent of performing organization’s personnel assigned full-time to project work	Virtually none	0-25%	15-60%	50-95%	85-100%
Who controls the project budget	Functional manager	Functional manager	Mixed	Project manager	Project manager
Project manager’s role	Part-time	Part-time	Full-time	Full-time	Full-time
Common title for project manager’s role	Project Coordinator/ Project Leader	Project Coordinator/ Project Leader	Project Manager/ Project Officer	Project Manager/ Program Manager	Project Manager/ Program Manager
Project management administrative staff	Part-time	Part-time	Part-time	Full-time	Full-time

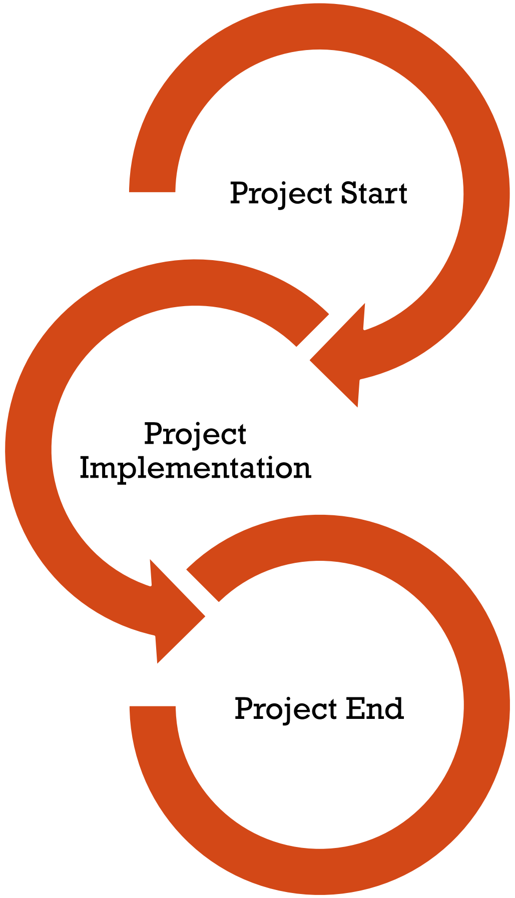
PMBOK® Guide, 2000, 19, and *PMBOK® Guide 2004*, 28.

ORGANIZATIONAL CULTURE

- **Organizational culture** is a set of shared assumptions, values, and behaviors that characterize the functioning of an organization
- Many experts believe that the underlying causes of many companies' problems are not the structure or staff, but the CULTURE ITSELF.

THE COMPONENT OF NETWORK SECURITY PROJECT MANAGEMENT

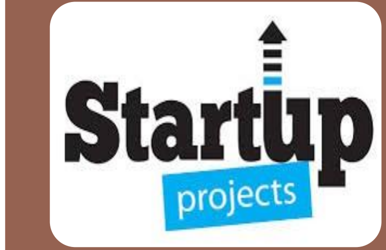
COMPONENT OF NETWORK SECURITY PROJECT MANAGEMENT -1



- NSPM involves project start, project implementation and project end.
- In project start consists of asset identification, assessment, analysis and policy construction.
- On the other hand, project implementation consists of architecture (topology), budget & cost, people & expertise and datelines.
- Meanwhile, in project end, the training and manual need to be hand over.

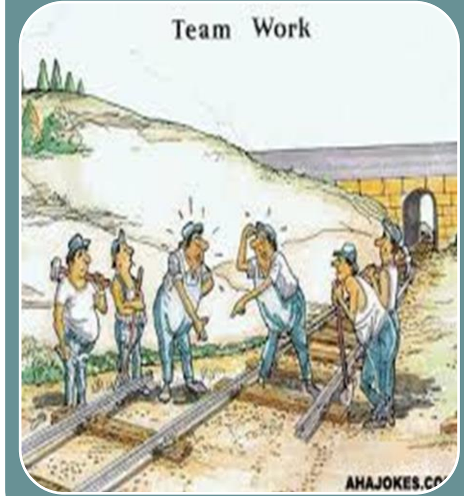
COMPONENT OF NETWORK SECURITY PROJECT MANAGEMENT - 2

Project Start (Initiation and Planning)



- Ice Breaking and Meetings
- Identification of Assets, Threats and Risks
- Assessment of Assets, Threats and Risks
- Analysis
- Policy Constructions
- Planning and Designing the Topologies (Logical & Physical)
- Work Breakdown Structure, PERT and Gantt Chart.

Project Implementation (Executing and Controlling)



Process Group / Expertise and Communication
Scope
Time
Budget / Cost
Quality
Procurement
Project Integration
Control and Datelines

Project End (Closing)

- Project and Report Hand Over
- Training / Warranty / License

PROJECT START

- Meetings
- Identification (Assets, Threats and Risks)
- Assessment (Assets, Threats and Risks)
- Planning and Designing
- Policy Construction
- WBS, PERT and Gantt CHART

PROJECT IMPLEMENTATION

- cost
- people
- time
- scope
- procurement
- quality
- integration

PROJECT END

report

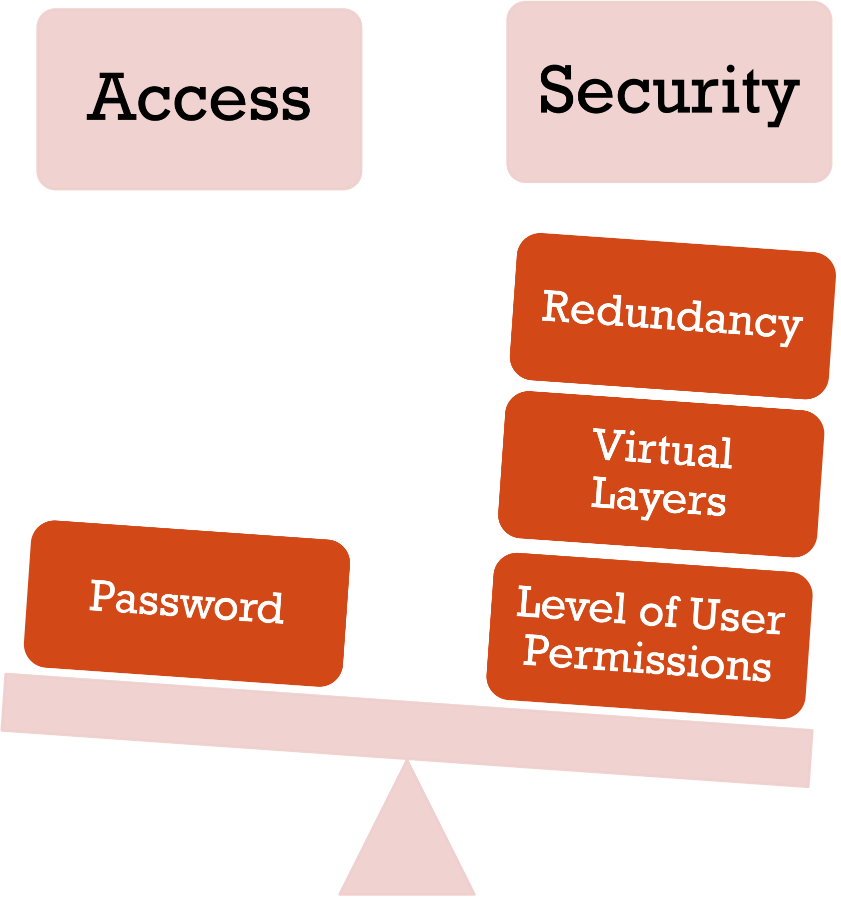
training

warranty

CONSTRAINTS/LIMITATIONS IN NETWORK SECURITY PROJECT MANAGEMENT

SECURITY CONSTRAINTS

- Cost of hardware and software : Becoming more and more expensive
- Either Security is Hardened or Access Lavish
- Internal and External Attacks and Threats
- Policy and Best Practice in the organization
- New type of computer virus



SECURITY PLANNING

CONSTRAINTS	PLANNINGS
Cost of hardware and software : more expensive	Alternative Solution (i.e. instead of CISCO) in purchasing the hardware and software product
Either Security is Hardened or Access Lavish	Balance in between security and access
Internal and External Attacks and Threats	Network Protection through IDS, Firewall, Routing and Switching Protocols
Policy and Best Practice in the organization	Planning on Policy Construction and Implementation

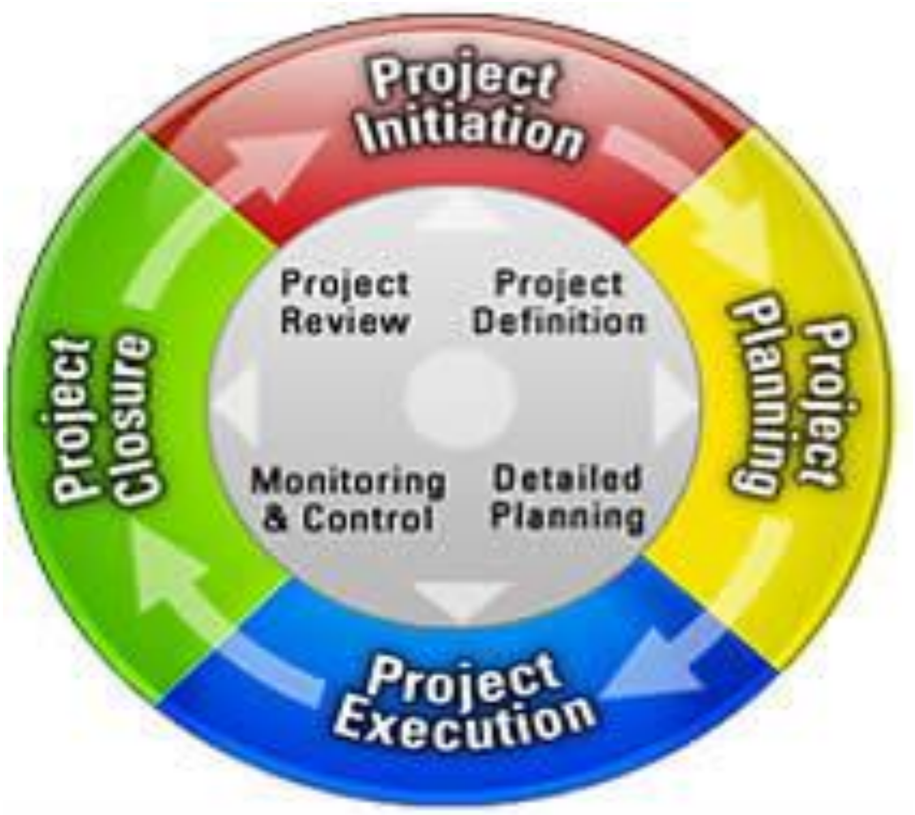
EXAMPLE OF SECURITY CONSTRAINT & PLANNING

Sections in the Plan	Description
Security risks	Enumerates the types of security hazards that affect your enterprise.
Security strategies	Describes the general security strategies necessary to meet the risks.
Public key infrastructure policies	Includes your plans for deploying certification authorities for internal and external security features.
Security group descriptions	Includes descriptions of security groups and their relationship to one another. This section maps group policies to security groups.
Group Policy	Includes how you configure security Group Policy settings, such as network password policies.
Network logon and authentication strategies	Includes authentication strategies for logging on to the network and for using remote access and smart card to log on.
Information security strategies	Includes how you implement information security solutions, such as secure e-mail and secure Web communications.
Administrative policies	Includes policies for delegation of administrative tasks and monitoring of audit logs to detect suspicious activity.

NETWORK SECURITY PROJECT MANAGEMENT PLAN DESCRIPTION

- Project Management Phase and Life Cycle
- Methodology of Network Security Project Management

PROJECT MANAGEMENT PHASE & LIFE CYCLE



- There are five phases in the project management lifecycle:
- Initiating
- Planning
- Executing
- Monitoring and controlling
- Closing

Source: PMBOK

METHODOLOGY FOR NSPM - SECURITY COST MODEL (SECOMO)

(JIHENE KRICHENE AND NOUREDDINE BOUDRIGA, 2007)

- First, a software project output is a product sailed to customers for a use purpose. For security projects, the output is a system including security policy, countermeasures installed on the network, and monitoring tools. The latter are also proper to security projects as they aim at controlling the network security state. Second, the complexity in software cost estimation depends on the software size, whereas in security projects, the complexity is related to the solution size, the heterogeneity of the network resources used by this solution, the interaction between them, and the extent to which they are distributed and visible to outsiders. Third, the factors influencing software development effort and security effort are not the same. For instance, attack frequency and factors which affect mainly the security project, have no effect on software projects. The SECOMO effort estimation, E, is expressed in Man × TimeUnit and formalized by the following equation: $E = a \times EAF \times S\ b$ where a is constant, EAF is an Effort Adjustment Factor based on effort multipliers, S is the solution size, and b represents scale factors. It is noticed that the estimation is based on cost drivers and on complexity of the solution size.

METHODOLOGY FOR NETWORK SECURITY PROJECT MANAGEMENT

- First Stage
  - Output:
  - security policy, countermeasures installed on the network, and monitoring tools. The latter are also proper to security projects as they aim at controlling the network security state.
- Second Stage
  - complexity in software cost estimation depends on the software size, whereas in security projects, the complexity is related to the solution size, the heterogeneity of the network resources used by this solution, the interaction between them, and the extent to which they are distributed and visible to outsiders.

- **SEcurity COst MOdel (secomo) (Jihene Krichene and Noureddine Boudriga, 2007)**

- Third Stage
  - The SECOMO effort estimation, E, is expressed in Man × TimeUnit and formalized by the following equation: E = a × EAF × S b where a is constant, EAF is an Effort Adjustment Factor based on effort multipliers, S is the solution size, and b represents scale factors. It is noticed that the estimation is based on cost drivers and on complexity of the solution size.

WHEN A PROJECT IS A FAILURE

A SUCCESSFUL OUTCOME OR PRODUCT COMES FROM A GOOD PROJECT PLANNING AND IMPLEMENTATION

SUMMARY

1) Chapter 1 explains on project management concepts and its application towards network security project environment.
2) The component and sub-components of network security project management need to be clearly defined.
3) The implementation of network security process need to be based on project phase, life cycle and actual methodology.