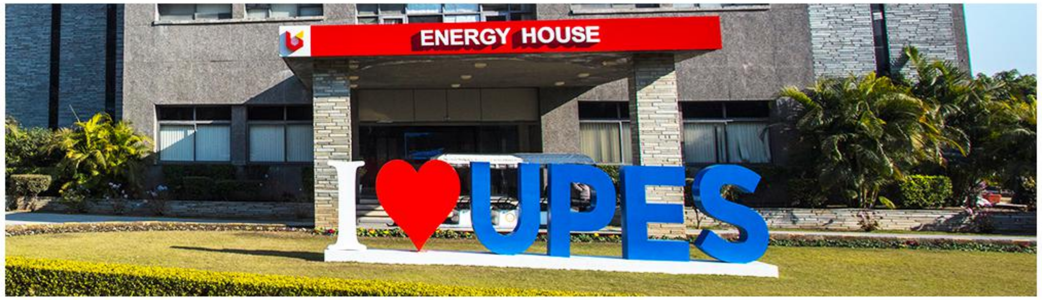


UPES

UNIVERSITY WITH A PURPOSE

Basics of Information Security

Objectives

- Understand the definition of information security
- Understand the key terms and concepts of information security
- Outline the phases of the security systems development life cycle
- Understand the roles of professionals involved in information security within an organization

Introduction

Information security: a “well-informed sense of assurance that the information risks and controls are in balance.” —Jim Anderson, Inovant (2002)

The Present

The Internet brings millions of computer networks into communication 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

What is Security?

“The quality or state of being secure—to be free from danger”

A successful organization should have multiple layers of security in place:

- Physical security
- Personal security
- Operations security
- Communications security
- Network security
- Information security

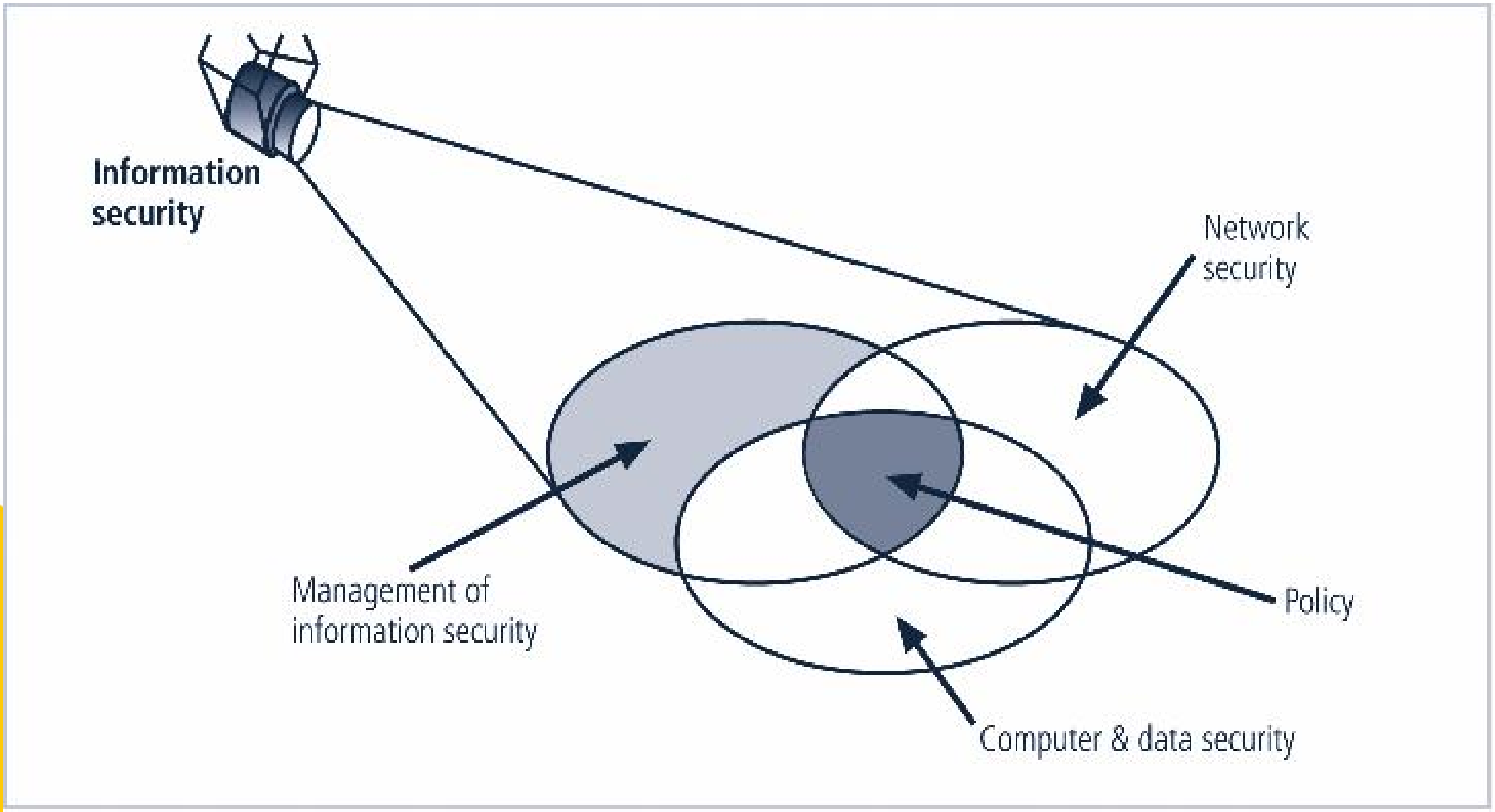
What is Information Security?

The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information

Necessary tools: policy, awareness, training, education, technology

C.I.A. triangle was standard based on confidentiality, integrity, and availability

C.I.A. triangle now expanded into list of critical characteristics of information



Components of Information Security

Critical Characteristics of Information

The value of information comes from the characteristics it possesses:

Availability

Accuracy

Authenticity

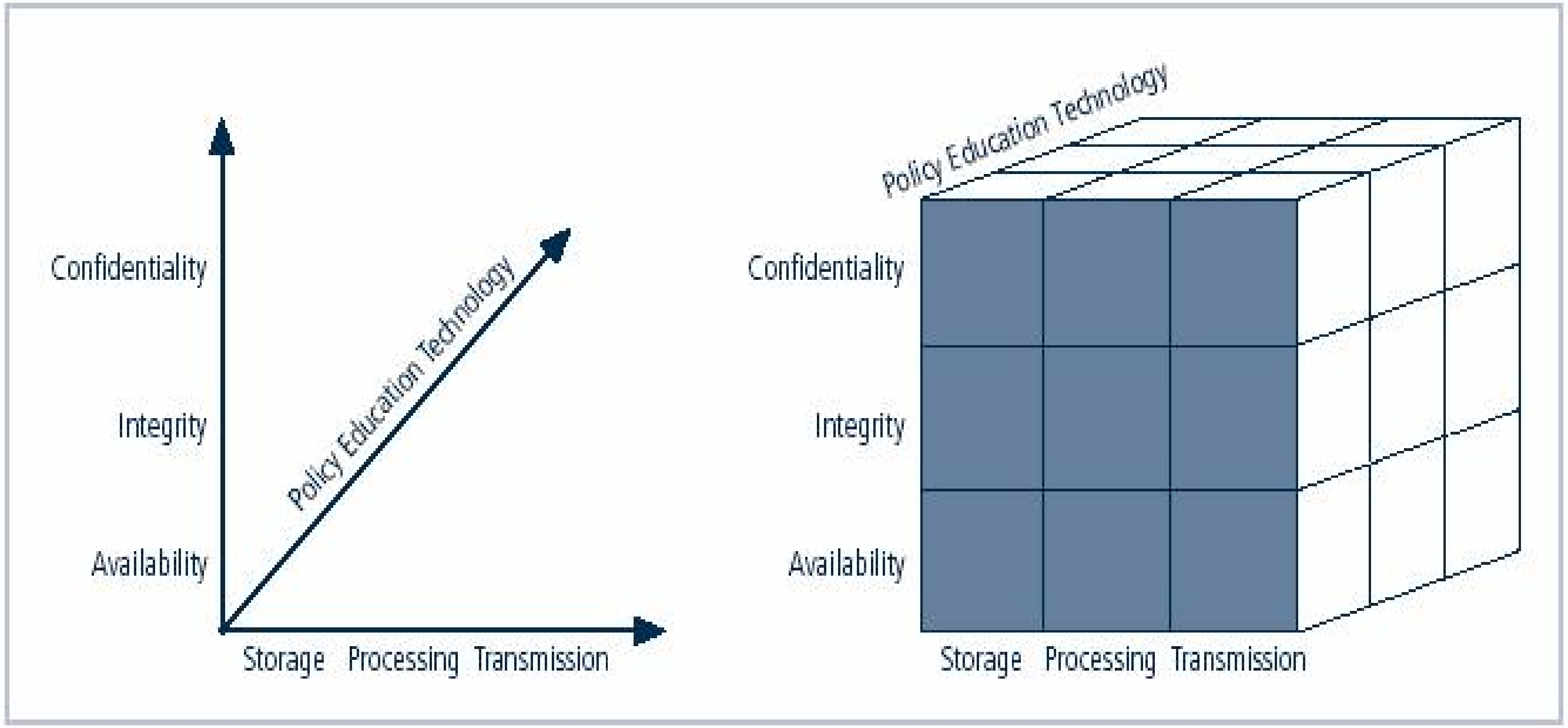
Confidentiality

Integrity

Utility

Possession

NSTISSC Security Model



NSTISSC Security Model

Components of an Information System

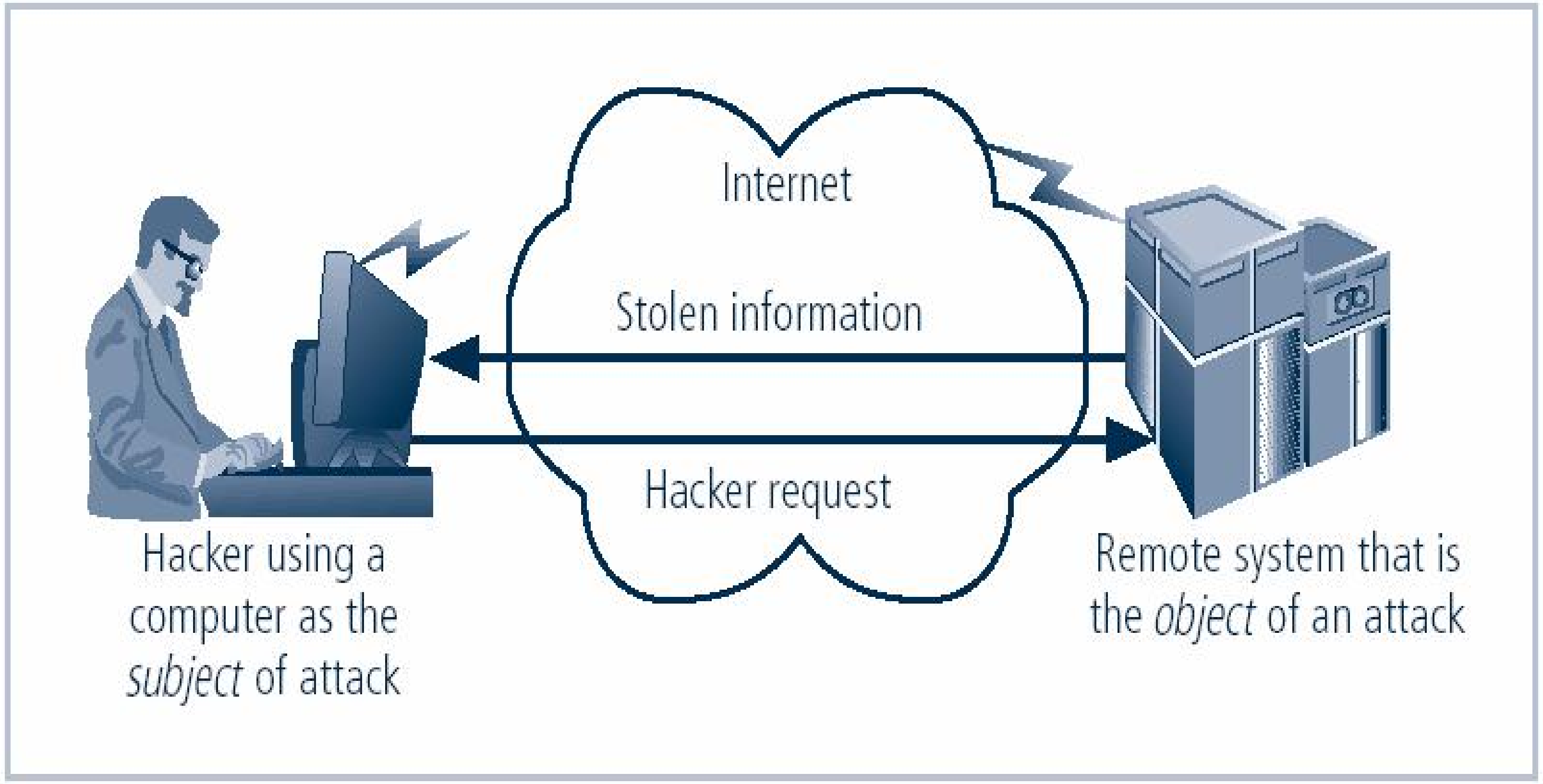
Information System (IS) is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization

Securing Components

Computer can be 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

When the object of an attack, computer is the entity being attacked


Internet
Stolen information
Hacker request
Hacker using a computer as the *subject* of attack
Remote system that is the *object* of an attack

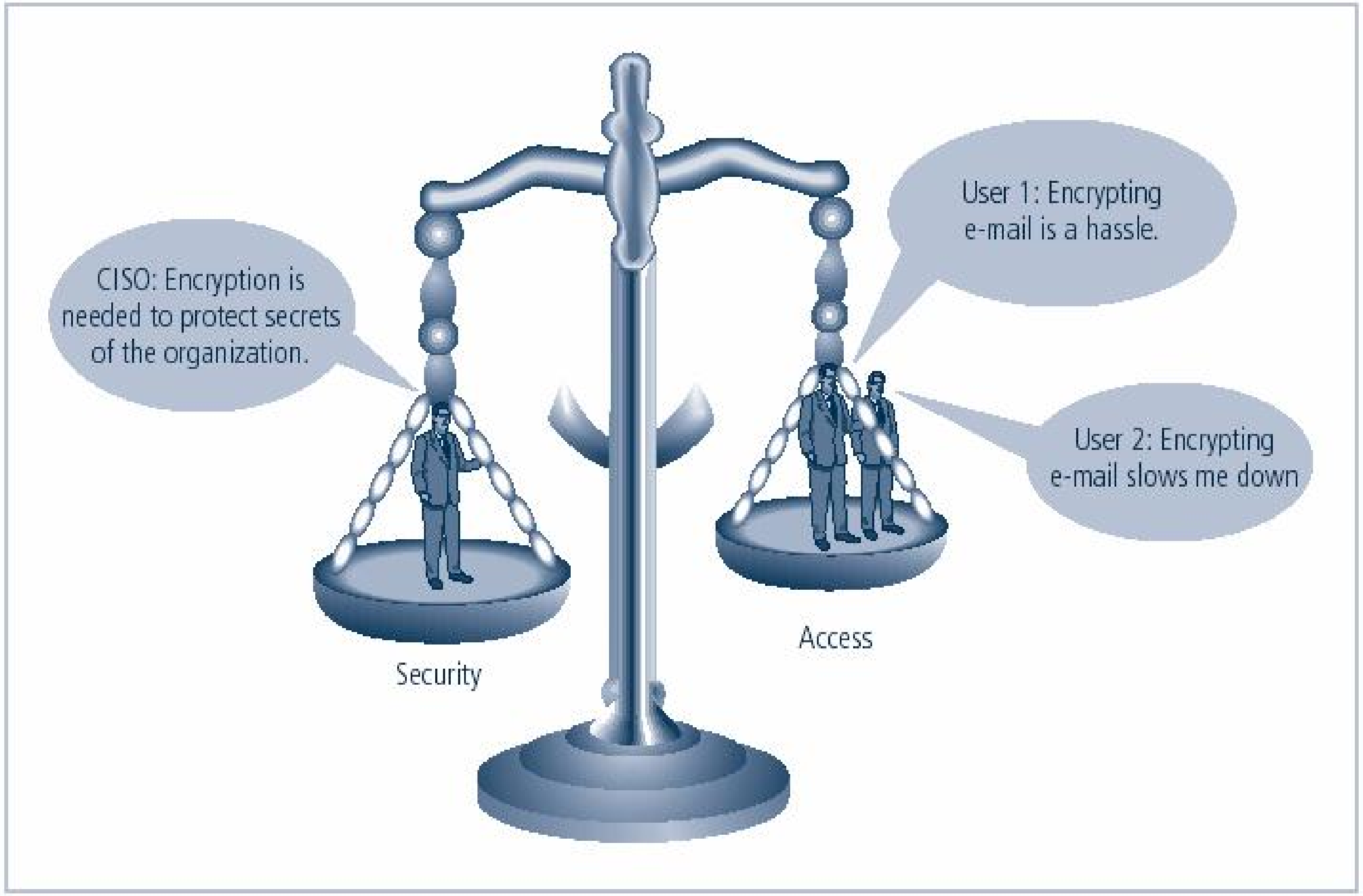
Computer as the Subject and Object of an Attack

Balancing Information Security and Access

Impossible to obtain perfect security—it is a process, not an absolute

Security should be considered balance between protection and availability

To achieve balance, level of security must allow reasonable access, yet protect against threats


CISO: Encryption is needed to protect secrets of the organization.
User 1: Encrypting e-mail is a hassle.
User 2: Encrypting e-mail slows me down
Security
Access

Balancing Information Security and Access

Approaches to Information Security Implementation: Bottom-Up Approach

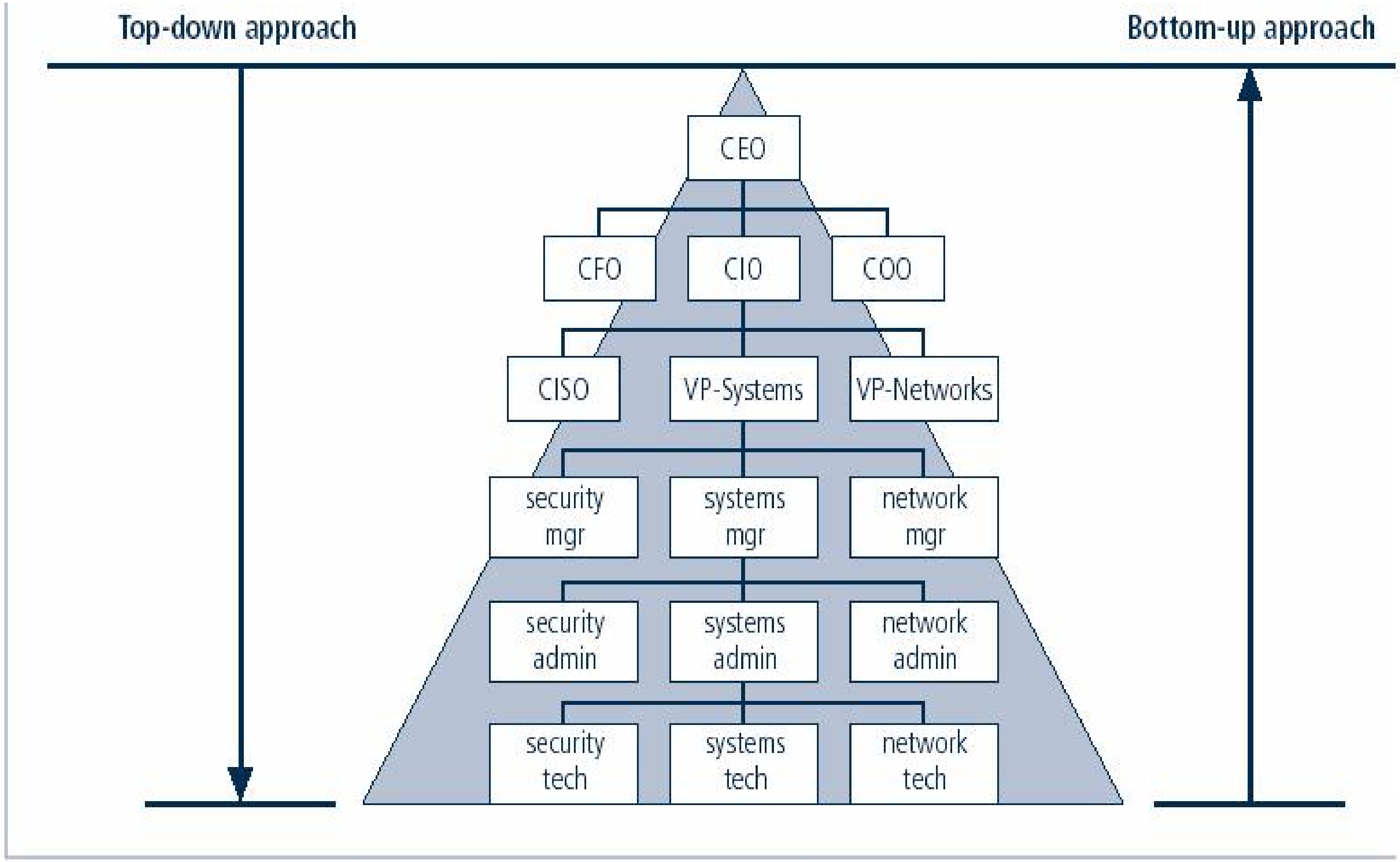
Grassroots effort: systems administrators attempt to improve security of their systems

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

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 also involve formal development strategy referred to as systems development life cycle

The Systems Development Life Cycle

Systems development life cycle (SDLC) is methodology and design for implementation of information security within an organization

Methodology is formal approach to problem-solving based on structured sequence of procedures

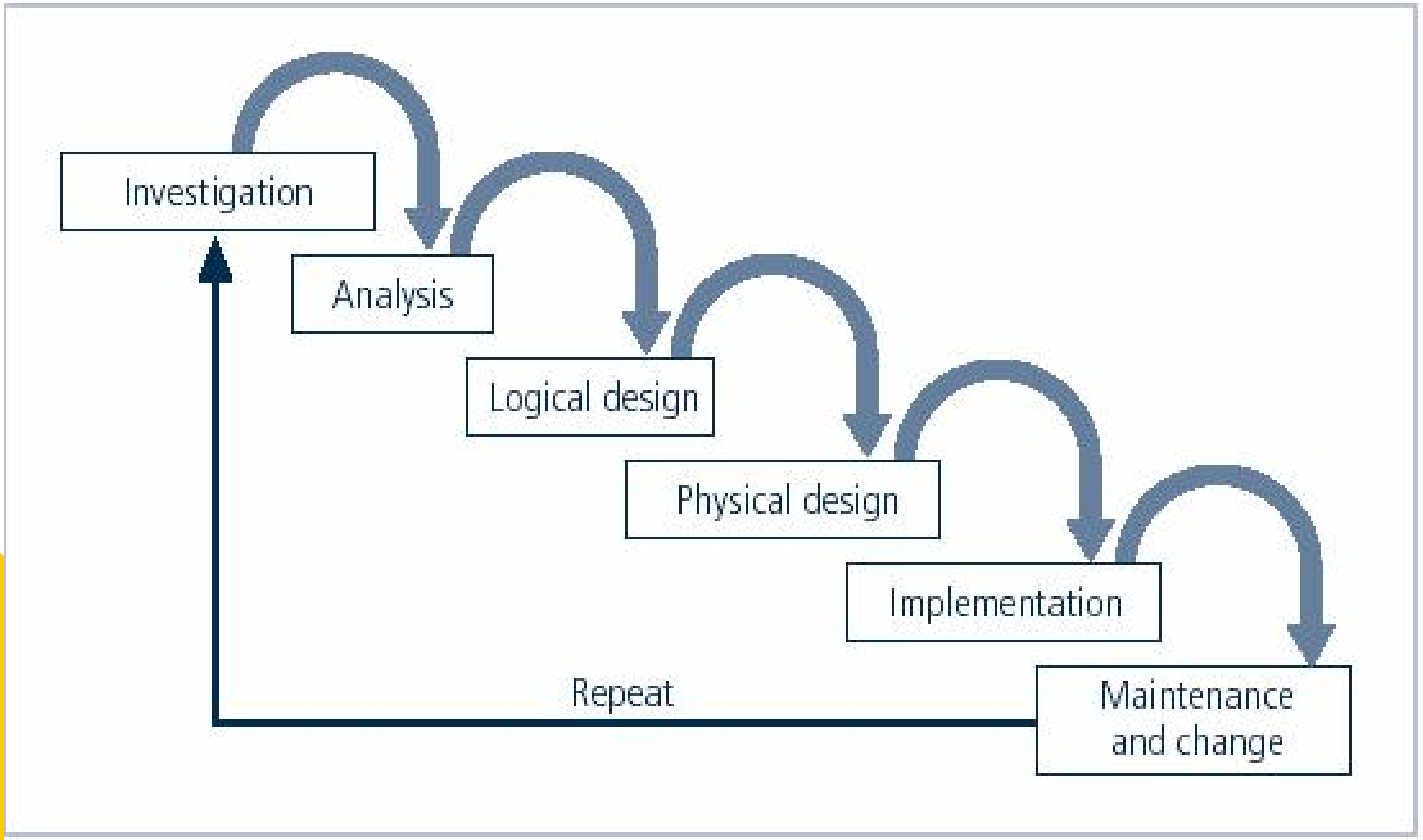
Using a methodology

ensures a rigorous process

avoids missing steps

Goal is creating a comprehensive security posture/program

Traditional SDLC consists of six general phases



SDLC Waterfall Methodology

Investigation

What problem is the system being developed to solve?

Objectives, constraints and scope of project are specified

Preliminary cost-benefit analysis is developed

At the end, feasibility analysis is performed to assesses economic, technical, and behavioral feasibilities of the process

Analysis

Consists of assessments of the organization, status of current systems, and capability to support proposed systems

Analysts determine what new system is expected to do and how it will interact with existing systems

Ends with documentation of findings and update of feasibility analysis

Logical Design

Main factor is business need; applications capable of providing needed services are selected

Data support and structures capable of providing the needed inputs are identified

Technologies to implement physical solution are determined

Feasibility analysis performed at the end

Physical Design

Technologies to support the alternatives identified and evaluated in the logical design are selected

Components evaluated on make-or-buy decision

Feasibility analysis performed; entire solution presented to end-user representatives for approval

Implementation

Needed software created; components ordered, received, assembled, and tested

Users trained and documentation created

Feasibility analysis prepared; users presented with system for performance review and acceptance test

Maintenance and Change

Consists of tasks necessary to support and modify system for remainder of its useful life

Life cycle continues until the process begins again from the investigation phase

When current system can no longer support the organization’s mission, a new project is implemented

The Security Systems Development Life Cycle

The same phases used in traditional SDLC may be adapted to support specialized implementation of an IS project

Identification of specific threats and creating controls to counter them

SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions

Investigation

Identifies process, outcomes, goals, and constraints of the project

Begins with enterprise information security policy

Organizational feasibility analysis is performed

Analysis

Documents from investigation phase are studied

Analyzes existing security policies or programs, along with documented current threats and associated controls

Includes analysis of relevant legal issues that could impact design of the security solution

The risk management task begins

Logical Design

Creates and develops blueprints for information security

Incident response actions planned:

Continuity planning

Incident response

Disaster recovery

Feasibility analysis to determine whether project should continue or be outsourced

Physical Design

Needed security technology is evaluated, alternatives generated, and final design selected

At end of phase, feasibility study determines readiness of organization for project

Implementation

Security solutions are acquired, tested, implemented, and tested again

Personnel issues evaluated; specific training and education programs conducted

Entire tested package is presented to management for final approval

Maintenance and Change

Perhaps the most important phase, given the ever-changing threat environment

Often, reparation and restoration of information is a constant duel with an unseen adversary

Information security profile of an organization requires constant adaptation as new threats emerge and old threats evolve

Security Professionals and the Organization

Wide range of professionals required to support a diverse information security program

Senior management is key component; also, additional administrative support and technical expertise required to implement details of IS program

Senior Management

Chief Information Officer (CIO)

Senior technology officer

Primarily responsible for advising senior executives on strategic planning

Chief Information Security Officer (CISO)

Primarily responsible for assessment, management, and implementation of IS in the organization

Usually reports directly to the CIO

Information Security Project Team

A number of individuals who are experienced in one or more facets of technical and non-technical areas:

Champion

Team leader

Security policy developers

Risk assessment specialists

Security professionals

Systems administrators

End users

Data Ownership

Data Owner: responsible for the security and use of a particular set of information

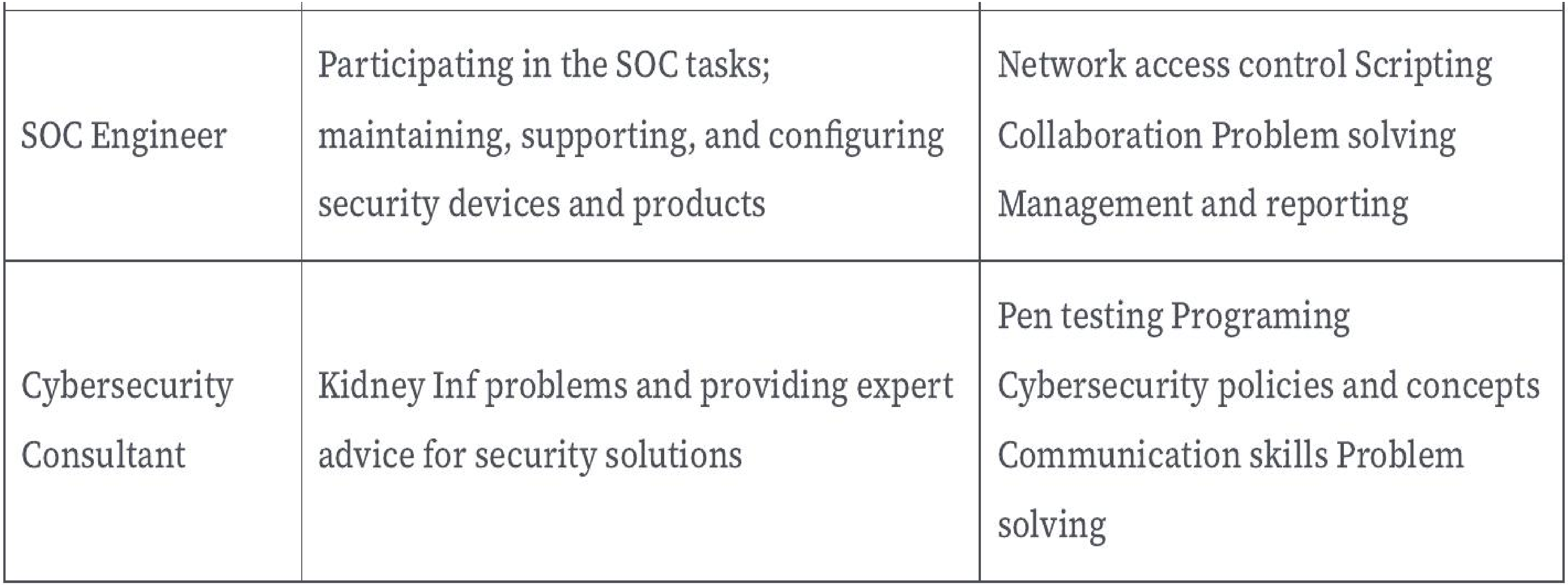
Data Custodian: responsible for storage, maintenance, and protection of information

Data Users: end users who work with information to perform their daily jobs supporting the mission of the organization

Role	Main Focus in the cyber security team	Essential Skills
CISO	Developing and implementing an information security program Establishing the right security governance plans Supervising different sectors in a cyber security team	Policy development and administration Strong technical background Strong communication skills Problem-solving
Cybersecurity Engineer	Designing, maintaining, and implementing highly secure network solutions	Secure coding practices Network architecture Ethical hacking Cybersecurity concepts and methodologies Problem solving
Cybersecurity Analyst	Identifying problems and developing plans to protect information from cyber threats and unauthorised access	Scripting Controls and frameworks Intrusion detection Networking Critical thinking Risk management

Cybersecurity Associate	Working to develop and implement a part of data security strategies	Security policies Network security systems Communication skills Strong research skills Analytical skills
Cybersecurity Responder	Responding and mitigating security incidents	Digital forensics Programming Investigation and analysis Collaboration Problem solving
Cybersecurity Incident Handler	Performing threat analysis and investigating security events according to the collected information	Analysis Network monitoring Troubleshooting Collaboration Problem solving
SOC Manager	Leading and managing the SOC team	Cybersecurity concepts and techniques Leadership Operational and management skills

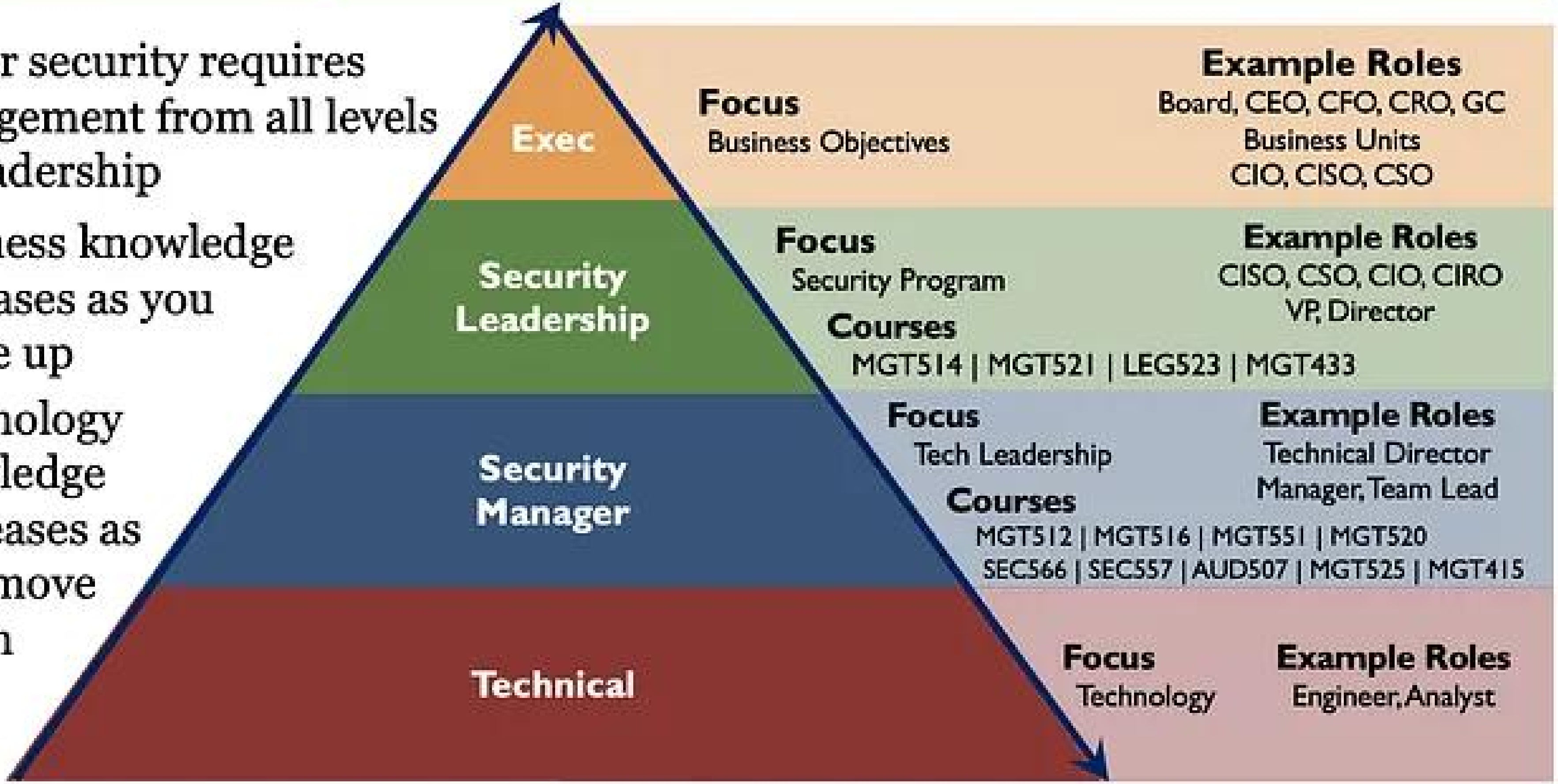
Security Director	Ensuring processes are aligned with the defined strategies and policies	Risk management and assessment Project management Cybersecurity policies and concepts
SecOps Lead	Leading and managing the SecOps team	Policies and concepts Risk management Communication skills
SOC Architect	Recognising the requirements and providing practical plans and security solutions	Cybersecurity concepts Network tools and devices Problem solving Time and project management
SIEM Engineer	Designing and developing solutions for the SIEM environment	Network security technologies Software development and scripting Problem solving



SOC Engineer	Participating in the SOC tasks; maintaining, supporting, and configuring security devices and products	Network access control Scripting Collaboration Problem solving Management and reporting
Cybersecurity Consultant	Kidney Inf problems and providing expert advice for security solutions	Pen testing Programing Cybersecurity policies and concepts Communication skills Problem solving

Cyber Leadership

- Cyber security requires engagement from all levels of leadership
- Business knowledge increases as you move up
- Technology knowledge increases as you move down



Exec

Focus
Business Objectives

Example Roles
Board, CEO, CFO, CRO, GC
Business Units
CIO, CISO, CSO

Security Leadership

Focus
Security Program

Courses
MGT514 | MGT521 | LEG523 | MGT433

Example Roles
CISO, CSO, CIO, CIRO
VP, Director

Security Manager

Focus
Tech Leadership

Courses
MGT512 | MGT516 | MGT551 | MGT520
SEC566 | SEC557 | AUD507 | MGT525 | MGT415

Example Roles
Technical Director
Manager, Team Lead

Technical

Focus
Technology

Example Roles
Engineer, Analyst

THANK YOU

UPES

UNIVERSITY WITH A PURPOSE