IT Security and Risk Management

Introduction

ا.د. حنان الطاهر الداقيز

h.dagez@uot.edu.ly

ربيع 2024

https://t.me/+xavNMXu7DyM5Yjc0

Introduction

- Some hundreds of years ago, we would have been making living on agriculture.
- Say a hundred years ago you were likely to be making a living working in a factory.
- Today, we live in the information age where everyone has a job somehow connected to information stored in digital form on a network.

History of Information Security

- Computer security began immediately after the first mainframes were developed

- Physical controls were needed to limit access to authorized personnel to sensitive military locations

The 1990s

- Networks of computers became more common, so too did the need to interconnect the networks
- Resulted in the Internet, the first manifestation of a global network of networks
- In early Internet deployments, security was treated as a low priority

The present

- The Internet has brought millions of computer networks into communication with each other – many of them unsecured
- Ability to secure each now influenced by the security on 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

Critical characteristics of information

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

Component of Information System

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

Approaches for implementing Security

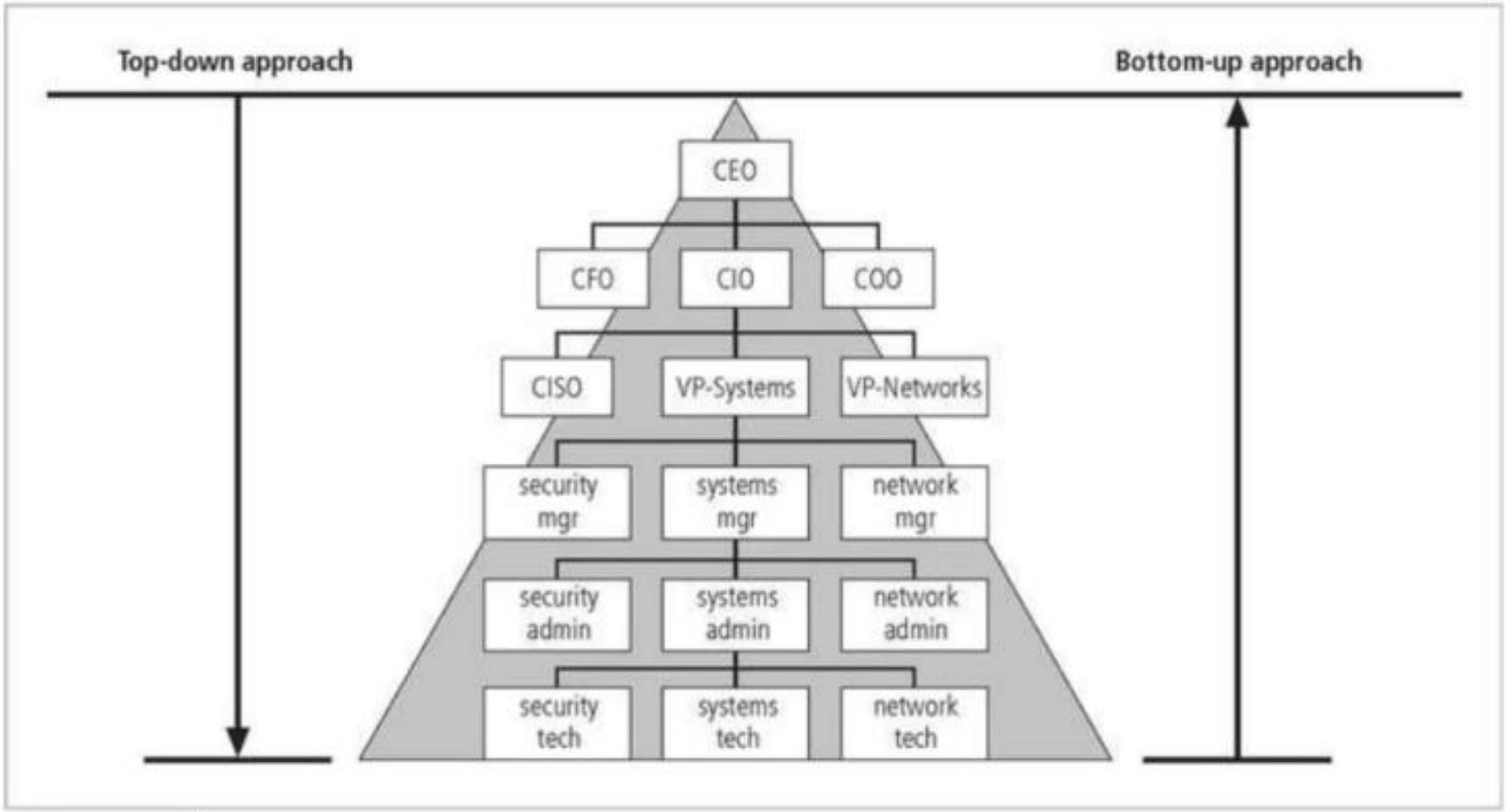
Bottom Up Approach

- Security from a grass-roots effort - systems administrators attempt to improve the security of their systems
- Key advantage - technical expertise of the individual administrators
- Seldom works, as it lacks a number of critical features:
  - participant support
  - organizational staying power

Top – Down Approach

- **Initiated by upper management:**
  - issue policy, procedures, and processes
  - dictate the goals and expected outcomes of the project
  - determine who is accountable for each of the required actions
- **This approach has strong upper management support, a dedicated champion, dedicated funding, clear planning, and the chance to influence organizational culture**
- **May also involve a formal development strategy referred to as a systems development life cycle**
  - Most successful top-down approach

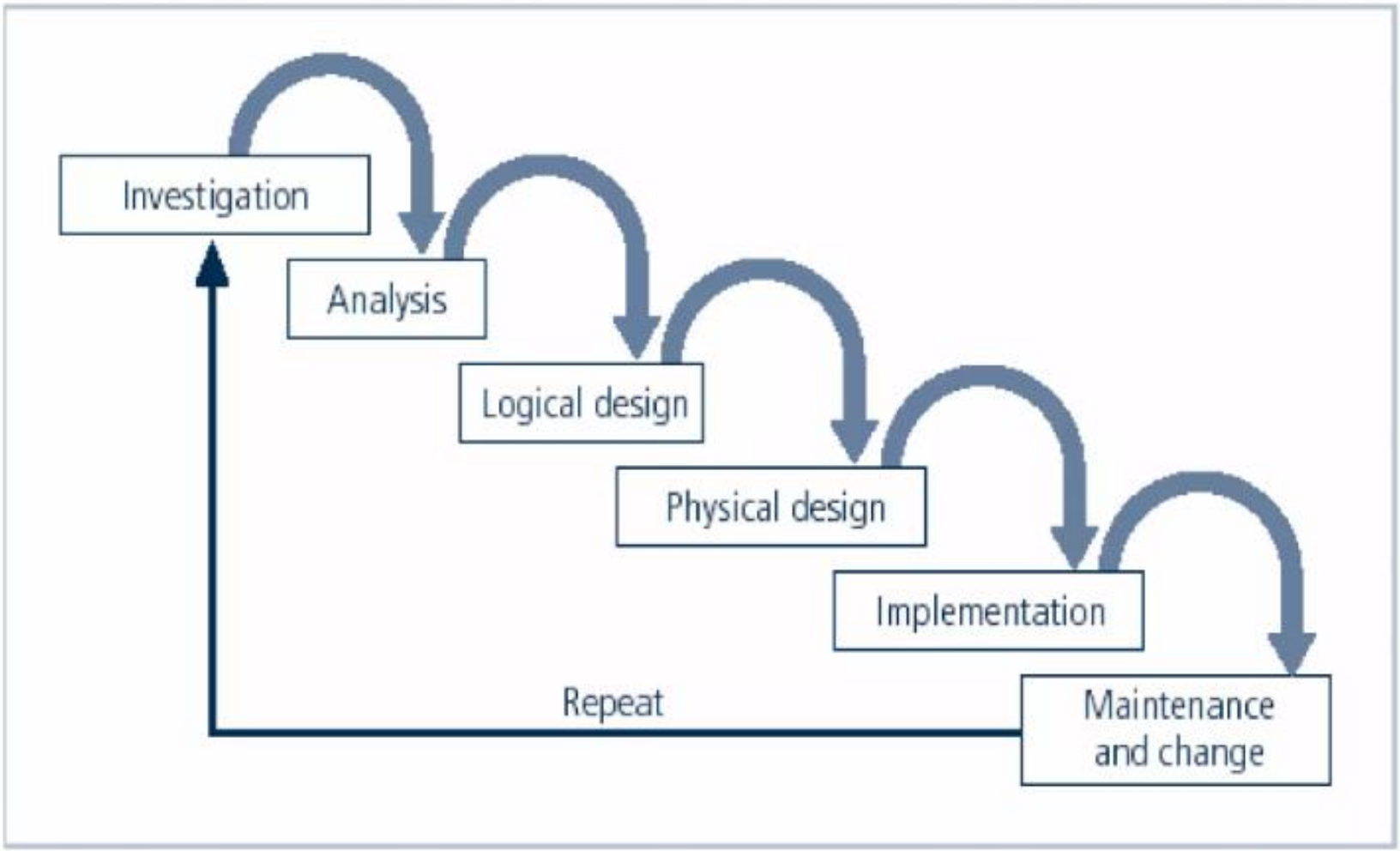
Approaches for implementing Security



Security Systems Development life cycle

- The same phases used in traditional SDLC may be adapte d to support specialized implementation of an IS project
  - Investigation
  - Analysis
  - Logical design
  - Physical design
  - Implementation
  - Maintenance & change
- Identification of specific threats and creating controls to counter them
- SecSDLC is a coherent program rather than a seri es of random, seemingly unconnected actions

SDLC



SDLC Waterfall Methodology

Investigation

- Identifies process, outcomes, goals, and const raints of the project
- Begins with enterprise information security po licy
- Organizational feasibility analysis is performed

Analysis

- Documents from investigation phase are studied
- Analyzes existing security policies or programs, a long with documented current threats and assoc iated controls
- Includes analysis of relevant legal issues that co uld 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

Professionals involved in information security within an organization

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, an d 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 required technical an d nontechnical areas:
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users