

Sixth Edition



INFORMATION SECURITY

PRINCIPLES OF INFORMATION SECURITY

[illegible]

Sixth Edition

Michael E. Whitman
Herbert J. Mattord

Learning Objectives

- Upon completion of this material, you should be able to:
 - Define information security
 - Recount the history of computer security and explain how it evolved into information security
 - Define key terms and critical concepts of information security
 - Explain the role of security in the systems development life cycle
 - Describe the information security roles of professionals within an organization

Introduction

- “Enterprise information security is a critical business capability that needs to be aligned with corporate expectations and culture that provides the leadership and insight to identify risks and implement effective controls.”—Martin Fisher, IT Security Manager, North side Hospital, Atlanta, Georgia
- Security professionals must review the origins of this field to understand its impact on our understanding of information security today

The History of Information Security

- Computer security began immediately after the first mainframes were developed
 - Groups developing code-breaking computations during World War II created the first modern computers.
 - Multiple levels of security were implemented.
- Physical controls limiting access to sensitive military locations to authorized personnel
- Rudimentary in defending against physical theft, espionage, and sabotage

Table 1-1 Key Dates in Information Security (1 of 2)

Date	Document
1968	Maurice Wilkes discusses password security in Time - Sharing Computer Systems.
1970	Willis H. Ware author the report Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security—RAND R.609 which was not declassified until 1979. It became known as the seminal work identifying the need for computer Security.
1973	Schell, Downey, and Popek examine the need for additional security in military systems in Preliminary Notes on the Design of Secure Military Computer Systems.
1975	The Federal Information Processing Standards (FIPS) examines DES (Digital Encryption Standard) In the Federal Register.
1978	Bisbey and Hollingsworth publish their study "Protection Analysis: Final Report," which discussed the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software.

Table 1-1 Key Dates in Information Security (2 of 2)

Date	Document
1979	Dennis Ritchie publishes "On the Security of UNIX" and "Protection of Data File Contents," which discussed secure user IDs, secure group IDs, and the problems inherent in the systems.
1982	The US. Department of Defense Computer Security Evaluation Center publishes the first version of the Trusted Computer Security (TCSEC) documents, which came to be known as the Rainbow Series.
1982	Grampp and Morris write "The UNIX System: UNIX Operating System Security." In this report the authors examined four "important handles to computer security": physical control of primes and computer facilities, management commitment to security objectives, education of employees, and administrative procedures aimed at increased security.
1984	Reeds and Weinberger publish "File Security and the UNIX System Crypt Command." Their premise was: "No technique can be secure against wiretapping or is equivalent on the computer. Therefore no technique can be secure against the system administrator or other privileged users... the naive user have no chance."
1992	Researchers for the Internet Engineering Task force, working at the Naval Research Laboratory, develop the Simple Internet Protocol Plus (SIPP) Security protocols, creating what is now known as IPSEC security.

Figure 1-1 The Enigma (1 of 2)



Source. Bletchley Park Trust. Used with permission.

Figure 1-1 The Enigma (2 of 2)

- Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or Unterseeboot version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. 'Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it'

The 1960s

- Advanced Research Projects Agency (ARPA) began to examine the feasibility of redundant networked communications.
- Larry Roberts developed the ARPANET from its inception.

Figure 1-2 Development of the ARPANET

ARPANET Program Plan
June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. Objectives – Develop Networking and Resource Sharing
2. Technical Need – Linking Computers
3. Military Need – Resource Sharing - Not Nuclear War
4. Prior Work – MIT-SDC experiment
5. Effect on ARPA – Link 17 Computer Research Centers, Network Research Plan - Develop IMP's and start 12/69
6. Cost – \$3.4 M for 68-71

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 523
Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Statement of the Program

The objective of this program is twofold: (1) To develop techniques and obtain experience in interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying SRI's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its resources to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user on program on any of the networked computers can utilize any program or subprogram available on any other computer without having to modify the remote program.

Source. Courtesy of Dr. Lawrence Roberts. Used with permission.

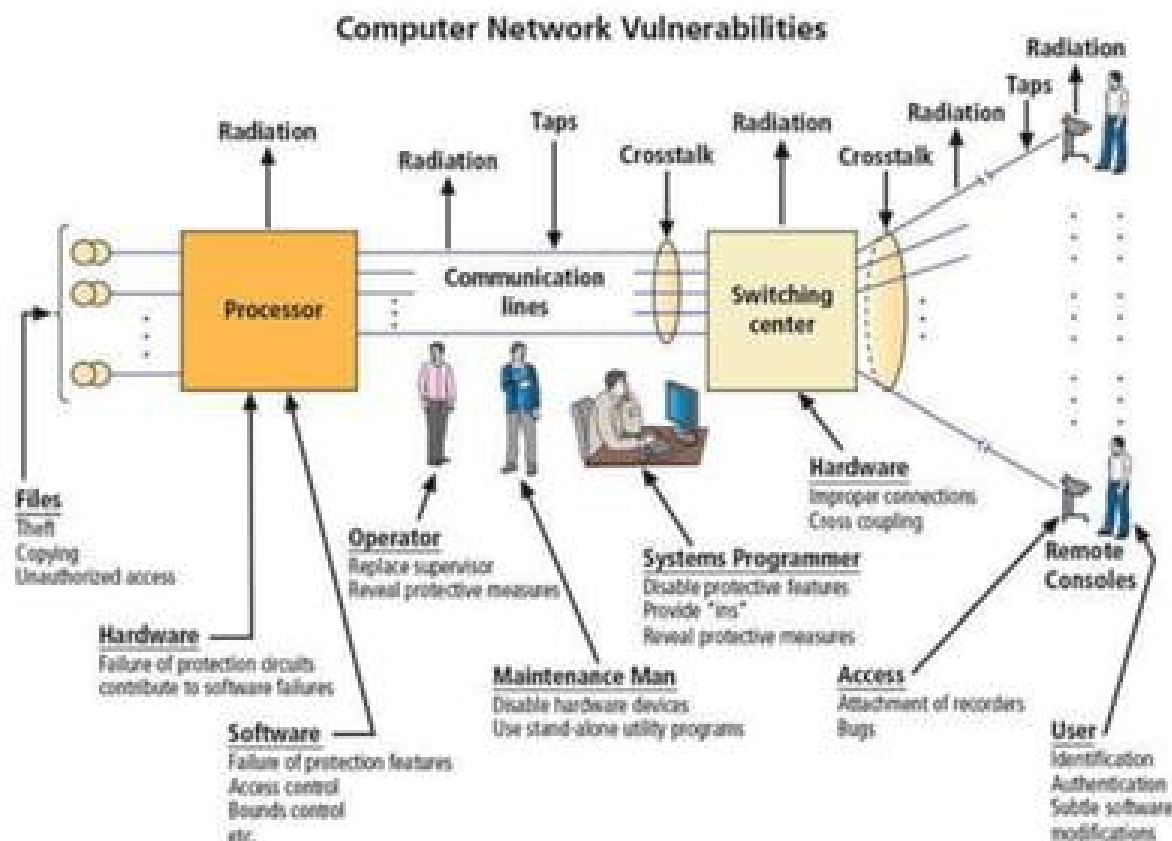
The 1970s and 80s (1 of 2)

- ARPANET grew in popularity, as did its potential for misuse.
- Fundamental problems with ARPANET security were identified.
 - No safety procedures for dial-up connections to ARPANET
 - Nonexistent user identification and authorization to system

The 1970s and 80s (2 of 2)

- Information security began with RAND Report R-609 (paper that started the study of computer security and identified the role of management and policy issues in it).
- The scope of computer security grew from physical security to include:
 - Securing the data
 - Limiting random and unauthorized access to data
 - Involving personnel from multiple levels of the organization in information security

Figure 1-4 Illustration of computer network vulnerabilities from RAND Report R-609



Source. RAND Report R-609-1. Used with permission.

MULTICS (1 of 2)

- Early focus of computer security research centered on a system called Multiplexed Information and Computing Service (MULTICS).
- First operating system was created with security integrated into core functions.
- Mainframe, time-sharing operating system was developed in the mid-1960s by General Electric (GE), Bell Labs, and Massachusetts Institute of Technology (MIT).

MULTICS (2 of 2)

- Several MULTICS key players created UNIX.
 - Primary purpose of UNIX was text processing.
- Late 1970s: The microprocessor expanded computing capabilities and security threats.

The 1990s

- Networks of computers became more common, as did the need to connect them to each other.
- Internet became the first global network of networks.
- Initially, network connections were based on de facto standards.
- In early Internet deployments, security was treated as a low priority.
- In 1993, DEFCON conference was established for those interested in information security.

2000 to Present

- The Internet brings millions of unsecured computer networks into continuous communication with each other.
- The ability to secure a computer's data was influenced by the security of every computer to which it is connected.
- Growing threat of cyber attacks has increased the awareness of need for improved security.
 - Nation-states engaging in information warfare

What Is Security? (1 of 2)

- “A state of being secure and free from danger or harm; the actions taken to make someone or something secure.”
- A successful organization should have multiple layers of security in place to protect:
 - Operations
 - Physical infrastructure
 - People
 - Functions
 - Communications
 - Information

What Is Security? (2 of 2)

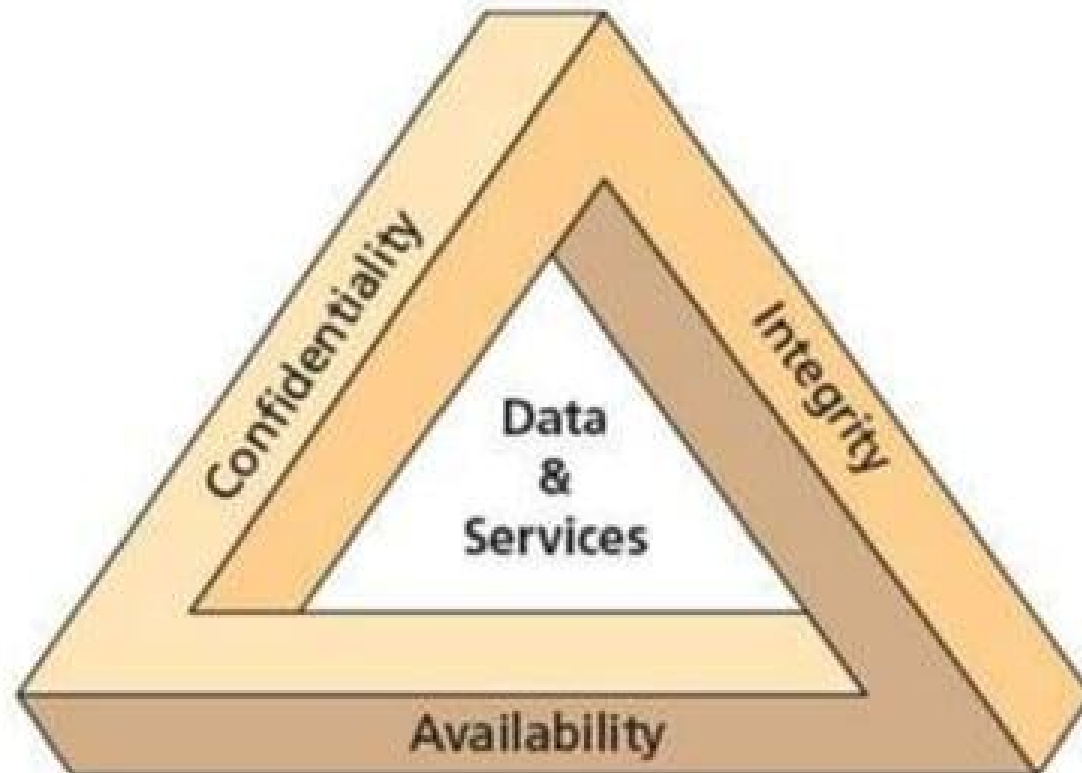
- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Includes information security management, data security, and network security
- C.I.A. triad
 - Is a standard based on confidentiality, integrity, and availability, now viewed as inadequate.
 - Expanded model consists of a list of critical characteristics of information.

Figure 1-5 Components of information security (1 of 2)



© Cengage Learning 2015

Figure 1-5 The C.I.A. triad (2 of 2)



© Cengage Learning 2015

Key Information Security Concepts (1 of 3)

- Access
- Asset
- Attack
- Control, safeguard, or countermeasure
- Exploit
- Exposure
- Loss
- Protection profile or security posture

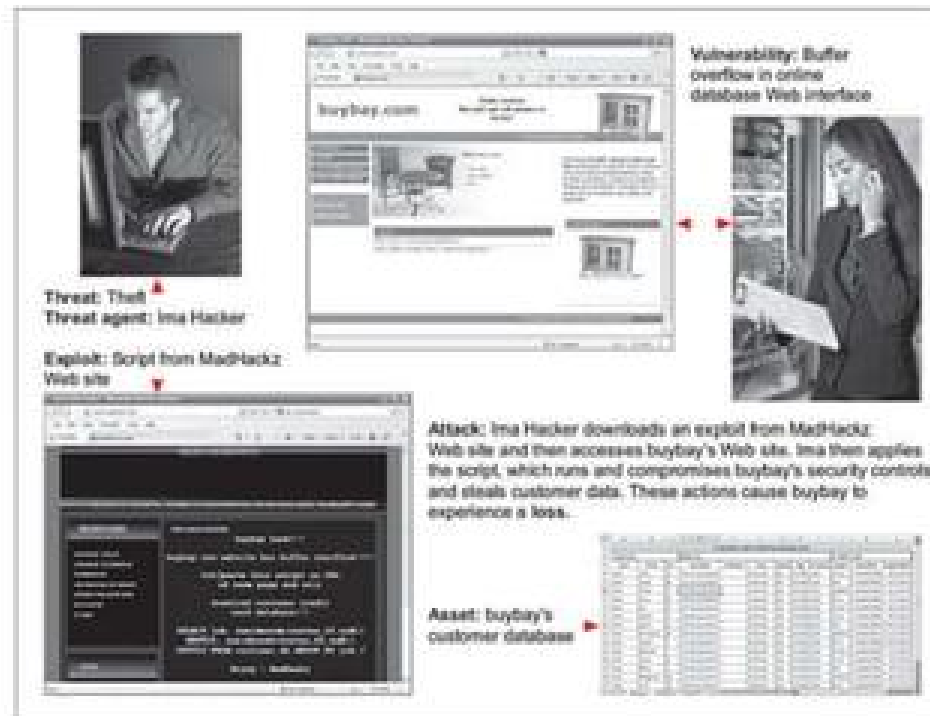
Key Information Security Concepts (2 of 3)

- Risk
- Subjects and objects of attack
- Threat
- Threat agent
- Threat event
- Threat source
- Vulnerability

Key Information Security Concepts (3 of 3)

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

Figure 1-7 Key concepts in information security

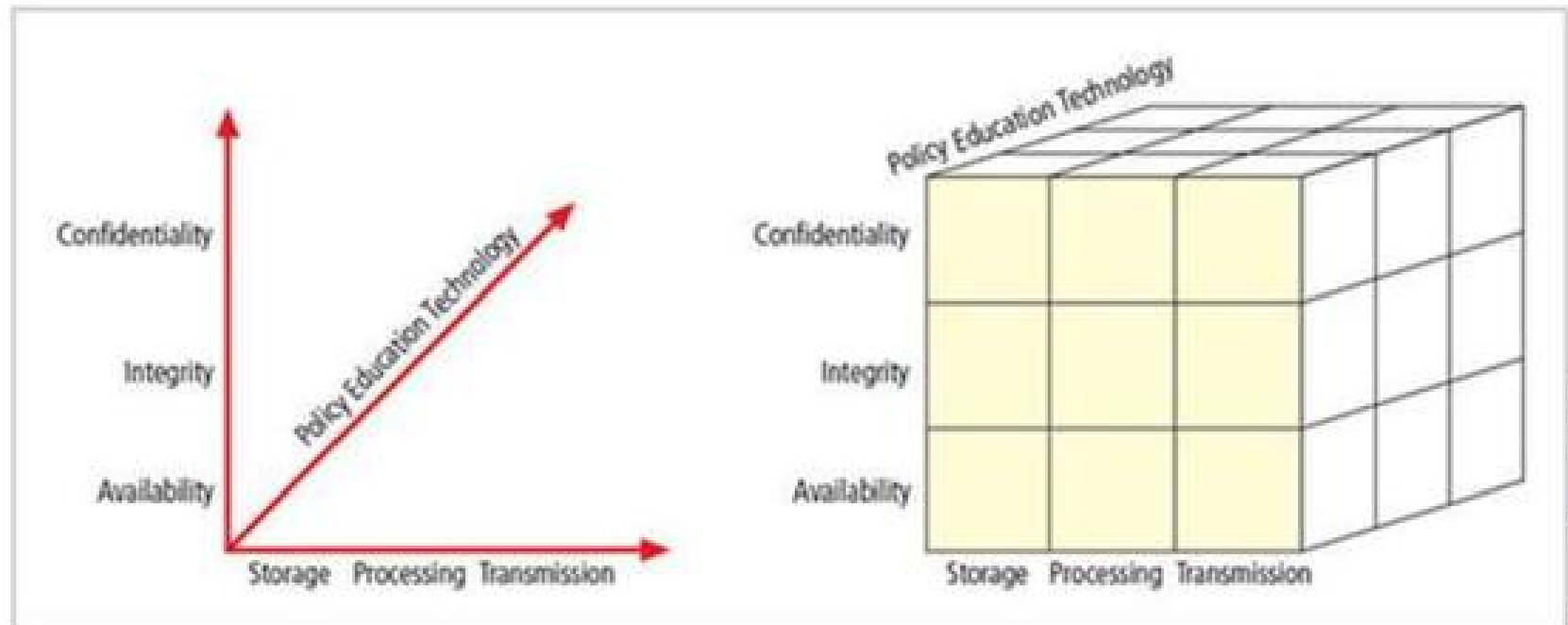


Source. (top left to bottom right): © iStockphoto/tadija, Internet Explorer, © iStockphoto/darrenwise, Internet Explorer, Microsoft Excel.

Critical Characteristics of Information

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

Figure 1-9 The McCumber Cube



© Cengage Learning 2015

Components of an Information System

- Information system (IS) is the entire set of people, procedures, and technology that enable business to use information.
 - Software
 - Hardware
 - Data
 - People
 - Procedures
 - Networks

Balancing Information Security and Access

- Impossible to obtain perfect information security—it is a process, not a goal.
- Security should be considered a balance between protection and availability.
- To achieve balance, the level of security must allow reasonable access, yet protect against threats.

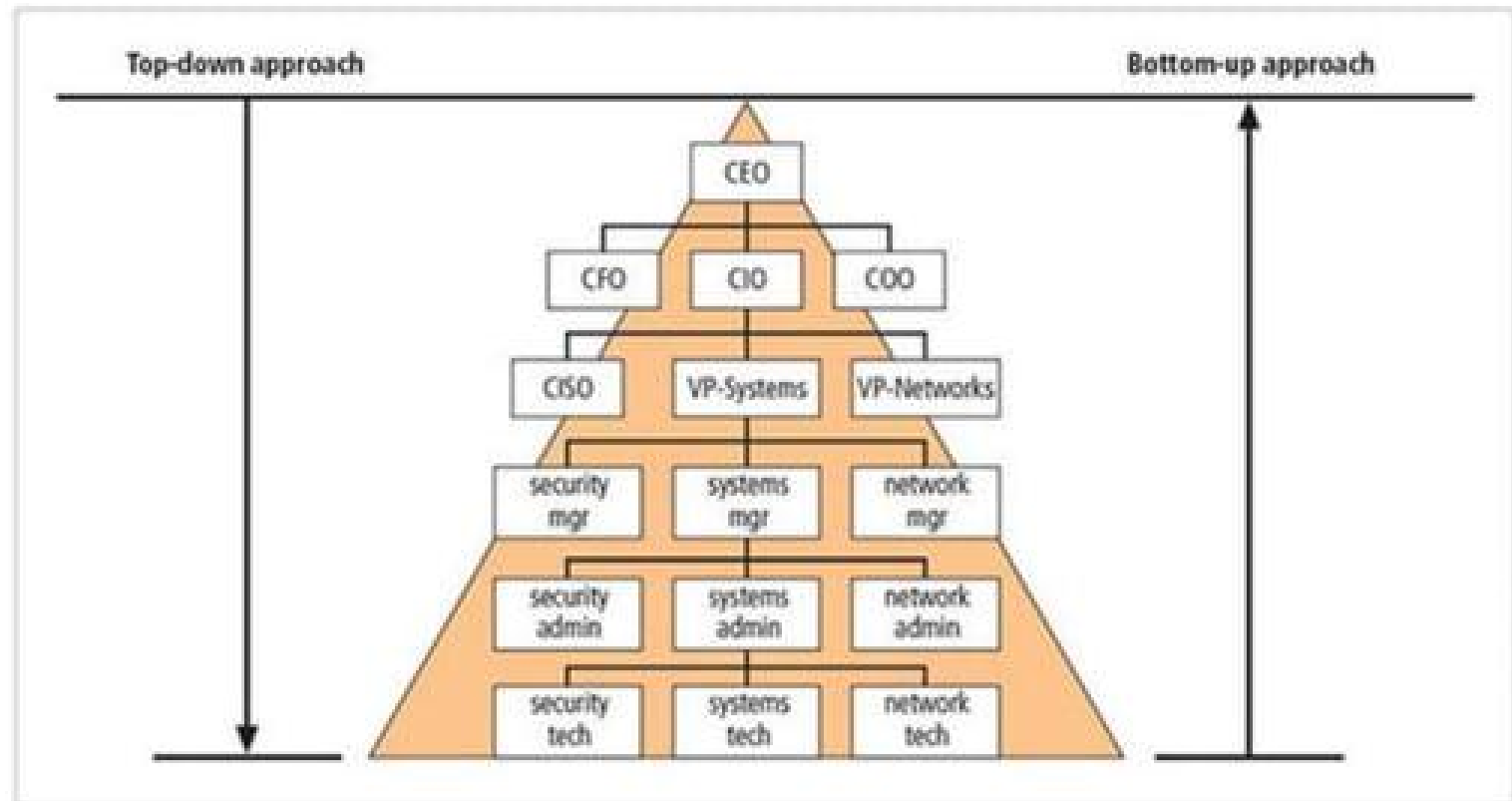
Approaches to Information Security Implementation: Bottom-Up Approach

- 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: 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 type of top-down approach also involves a formal development strategy referred to as systems development life cycle.

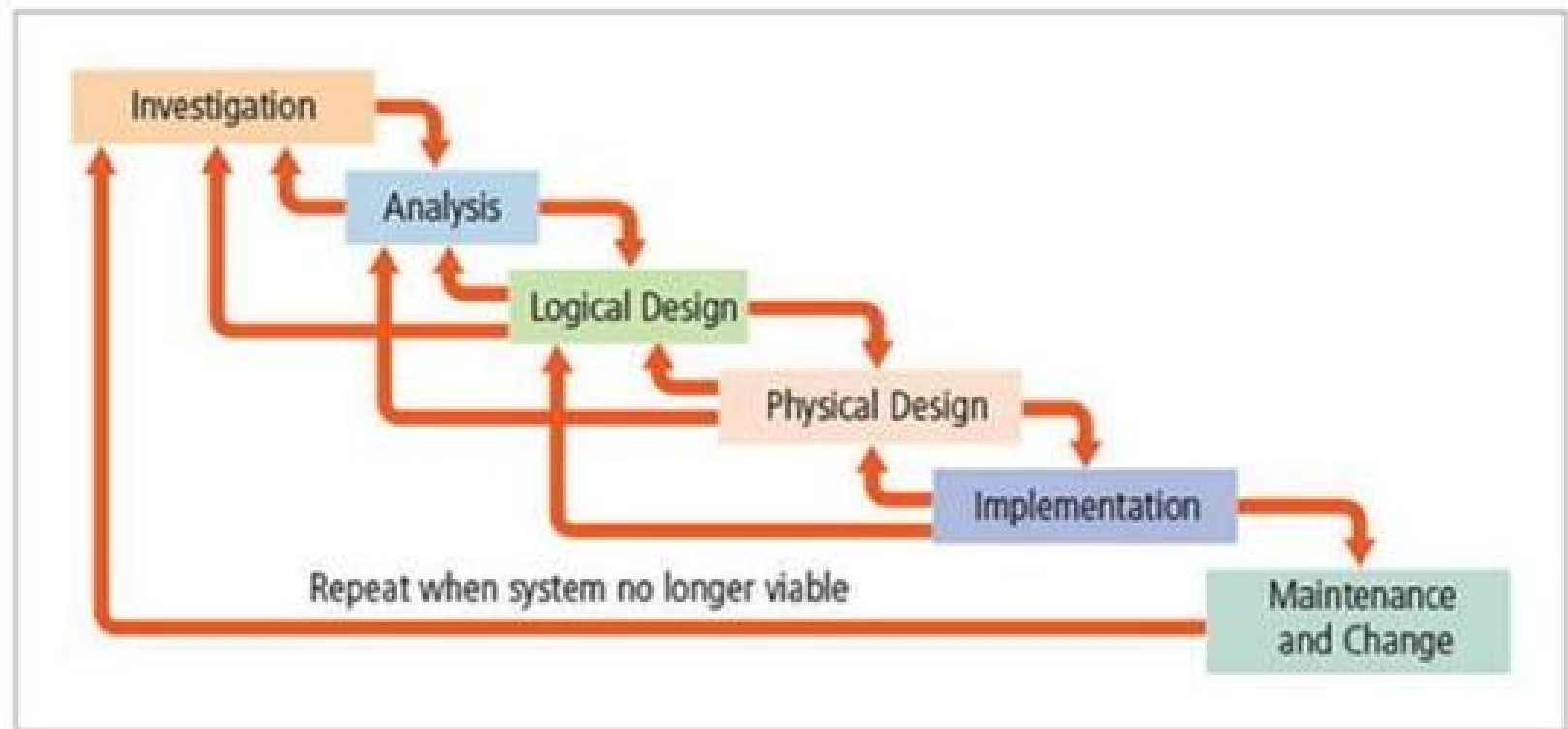
Figure 1-12 Approaches to information security implementation



Security in the Systems Development Life Cycle

- Systems development life cycle (SDLC): a methodology for the design and implementation of an information system
- Methodology: a formal approach to solving a problem based on a structured sequence of procedures
- Using a methodology:
 - Ensures a rigorous process with a clearly defined goal
 - Increases probability of success

Figure 1-13 SDLC waterfall methodology



© Cengage Learning 2015

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 of all phases, a process is undertaken to assess economic, technical, and behavioral feasibilities and ensure implementation is worth the time and effort.

Analysis

- Consists of assessments of:
 - The organization
 - Current systems
 - Capability to support proposed systems
- Analysts determine what the new system is expected to do and how it will interact with existing systems.
- Analysis ends with documentation of findings and an update of feasibility.

Logical Design

- The first and driving factor is the business need.
 - Applications are selected to provide needed services.
- Data support and structures capable of providing the needed inputs are identified.
- Specific technologies are delineated to implement the physical solution.
- Analysts generate estimates of costs and benefits to allow comparison of available options.
- Feasibility analysis is performed at the end.

Physical Design

- Specific technologies are selected to support the alternatives identified and evaluated in the logical design.
- Selected components are evaluated on make-or-buy decision.
- Feasibility analysis is performed.
- Entire solution is presented to organization's management for approval.

Implementation

- Needed software is created.
- Components are ordered, received, and tested.
- Users are trained and supporting documentation created.
- Feasibility analysis is prepared.
 - Sponsors are presented with the system for a performance review and acceptance test.

Maintenance and Change

- Longest and most expensive phase
- Consists of the tasks necessary to support and modify the system for the remainder of its useful life
- Life cycle continues until the team determines the process should begin again from the investigation phase
- When current system can no longer support the organization's mission, a new project is implemented

Software Assurance (1 of 3)

- Many organizations recognize the need to include planning for security objectives in the SDLC used to create systems.
 - Established procedures to create software that is more capable of being deployed in a secure fashion
- This approach is known as software assurance (SA).
- A national effort is under way to create a common body of knowledge focused on secure software development.

Software Assurance (2 of 3)

- U.S. Department of Defense and Department of Homeland Security supported the Software Assurance Initiative, which resulted in the publication of Secure Software Assurance (SwA) Common Body of Knowledge (CBK).
- SwA CBK serves as a strongly recommended guide to developing more secure applications.
- SwA CBK, which is a work in progress, contains the following sections:
 - Nature of Dangers
 - Fundamental Concepts and Principles
 - Ethics, Law, and Governance

Software Assurance (3 of 3)

- Secure Software Requirements
- Secure Software Design
- Secure Software Construction
- Secure Software Verification, Validation, and Evaluation
- Secure Software Tools and Methods
- Secure Software Processes
- Secure Software Project Management
- Acquisition of Secure Software
- Secure Software Sustainment

Software Design Principles (1 of 2)

Good software development results in secure products that meet all design specifications.

- Some commonplace security principles
 - Keep design simple and small
 - Access decisions by permission not exclusion
 - Every access to every object checked for authority
 - Design depends on possession of keys/passwords
 - Protection mechanisms require two keys to unlock
 - Programs/users utilize only necessary privileges

Software Design Principles (2 of 2)

- Some commonplace security principles
 - Minimize mechanisms common to multiple users
 - Human interface must be easy to use so users routinely/automatically use protection mechanisms.

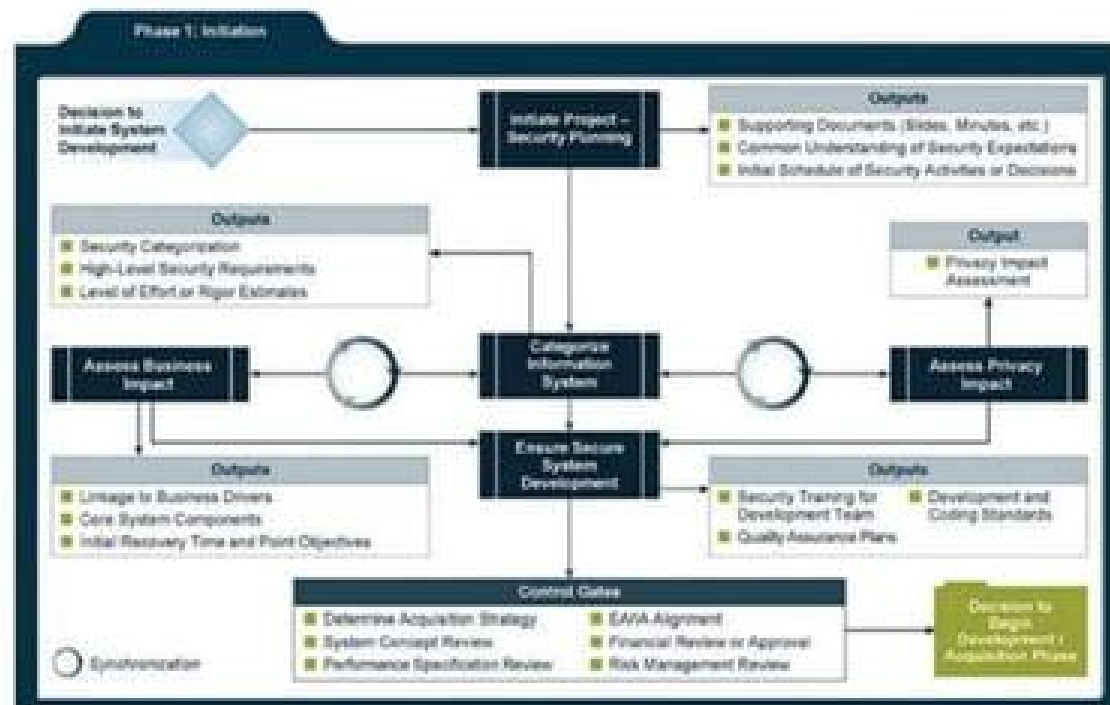
The NIST Approach to Securing the SDLC

- NIST Special Publication 800-64, rev. 2, maintains that early integration of security in the SDLC enables agencies to maximize return on investment through:
 - Early identification and mitigation of security vulnerabilities and misconfigurations
 - Awareness of potential engineering challenges
 - Identification of shared security services and reuse of security strategies and tools
 - Facilitation of informed executive decision making

The NIST Approach: Initiation

- Security at this point is looked at in terms of business risks, with information security office providing input.
- Key security activities include:
 - Delineation of business requirements in terms of confidentiality, integrity, and availability
 - Determination of information categorization and identification of known special handling requirements to transmit, store, or create information
 - Determination of any privacy requirements

Figure 1-14 Relating security considerations in the Initiation phase

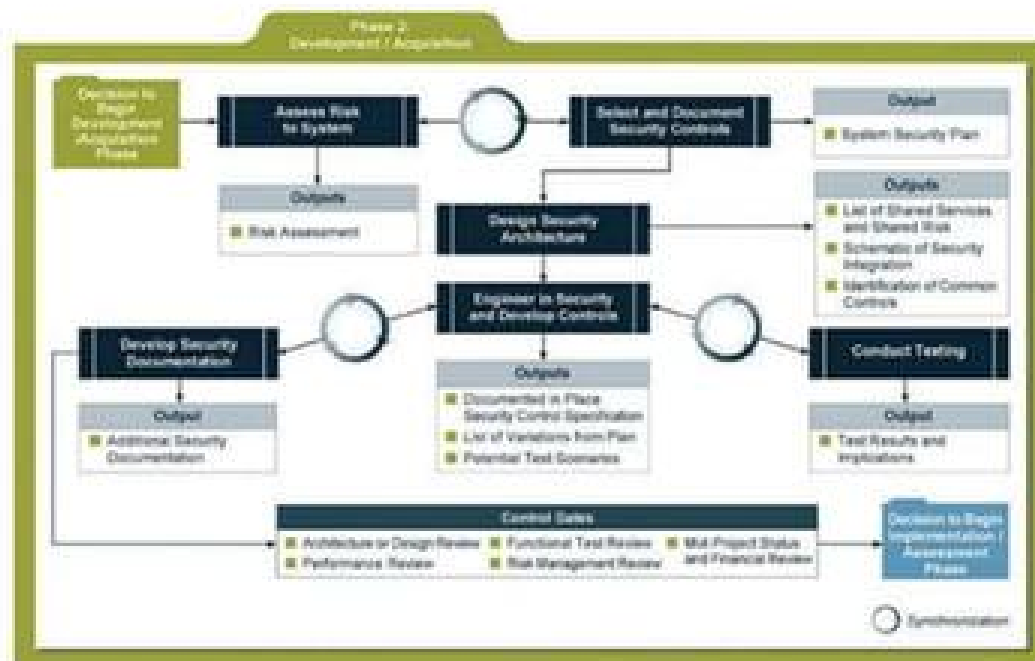


Source: NIST SP 800-64 Rev. 2: Security Considerations in the System Development Life Cycle.

The NIST Approach: Development/Acquisition

- Key security activities include:
 - Conducting risk assessment and using results to supplement baseline security controls
 - Analyzing security requirements
 - Performing functional and security testing
 - Preparing initial documents for system certification and accreditation
 - Designing security architecture

Figure 1-15 Relating security considerations in the Development/Acquisition phase

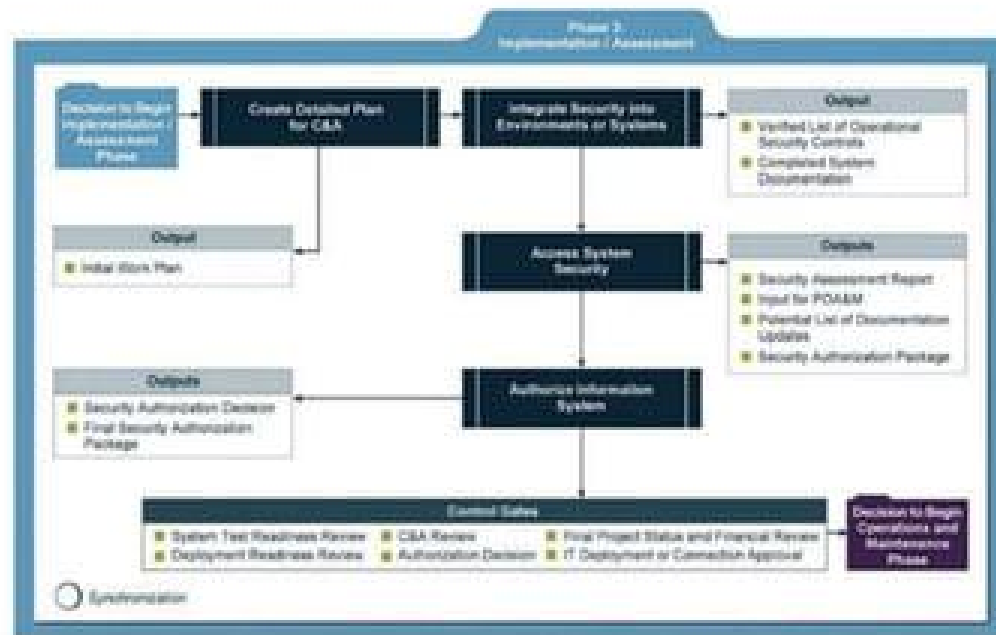


Source: NIST SP 800-64 Rev. 2: Security Considerations in the System Development Life Cycle.

The NIST Approach: Implementation/Assessment

- System is installed and evaluated in operational environment.
- Key security activities include:
 - Integrating information system into its environment
 - Planning and conducting system certification activities in synchronization with testing of security controls
 - Completing system accreditation activities

Figure 1-16 Relating security considerations in the Implementation/Assessment phase

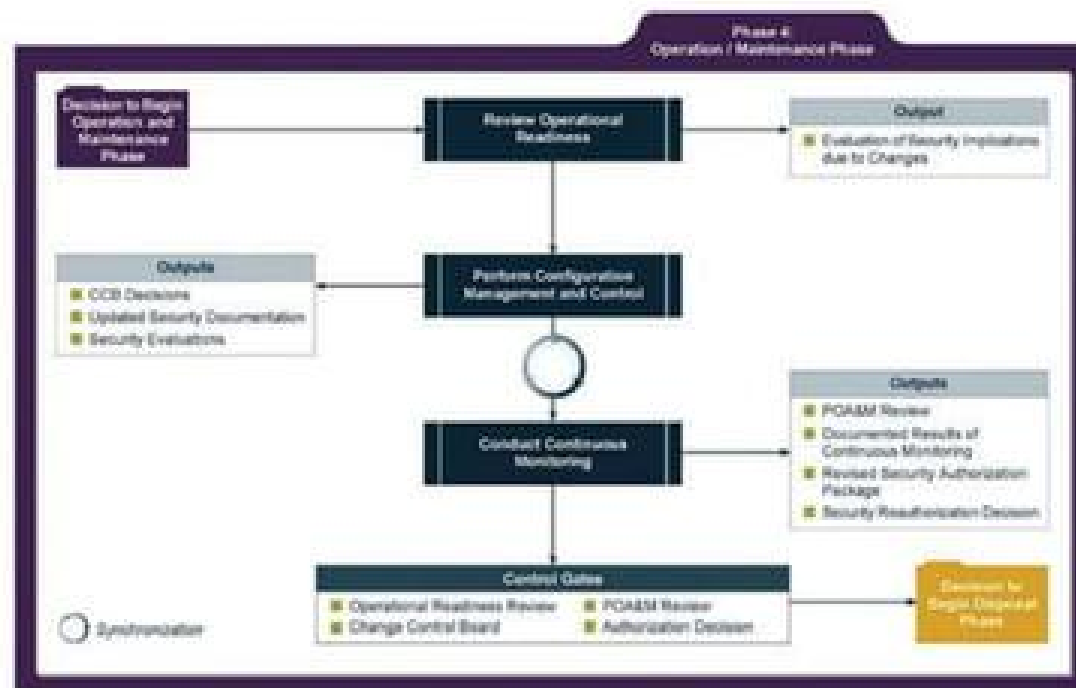


Source: NIST SP 800-64 Rev. 2: Security Considerations in the System Development Life Cycle.

The NIST Approach: Operations and Maintenance

- Systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software are added or replaced.
- Key security activities include:
 - Conducting operational readiness review
 - Managing configuration of system
 - Instituting process and procedure for assured operations and continuous monitoring of information system's security controls
 - Performing reauthorization as required

Figure 1-17 Relating security considerations in the Operation/Maintenance phase

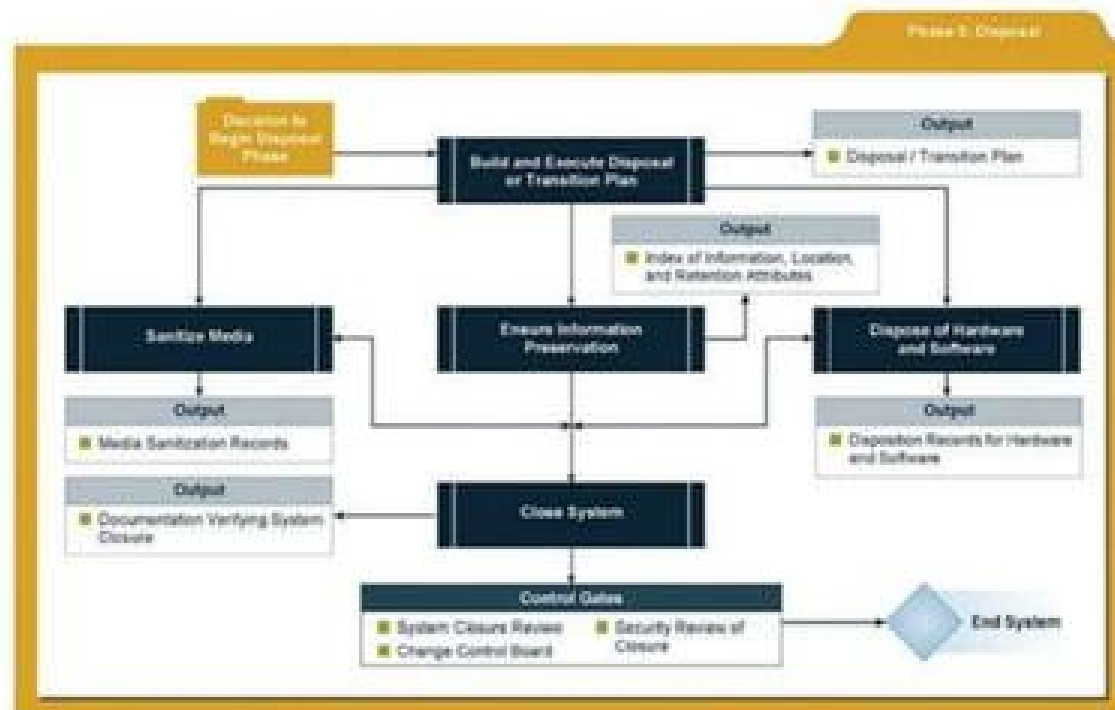


Source: NIST SP 800-64 Rev. 2: Security Considerations in the System Development Life Cycle.

The NIST Approach: Disposal

- Provides for disposal of system and closeout of any contracts in place
- Key security activities include:
 - Building and executing disposal/transition plan
 - Archival of critical information
 - Sanitization of media
 - Disposal of hardware and software

Figure 1-18 Relating security considerations in the Disposal phase



Source: NIST SP 800-64 Rev. 2: Security Considerations in the System Development Life Cycle.

Figure 1-19 Microsoft's SDL (1 of 3)

- Training:
 - Core security training
- Requirements:
 - Establish security requirements
 - Create quality gates/bug bars
 - Perform security and privacy risk assessments
- Design:
 - Establish design requirements
 - Perform attack surface analysts/ reduction
 - Use threat modeling

Figure 1-19 Microsoft's SDL (2 of 3)

- Implementation:
 - Use approved tools
 - Deprecate unsafe functions
 - Perform static analysis
- Verification:
 - Perform dynamic analysis
 - Perform fuzz testing
 - Conduct attack surface review

Figure 1-19 Microsoft's SDL (3 of 3)

- Release:
 - Create an incident response plan
 - Conduct nal security review
 - Certify release and archive
- Response:
 - Execute incident response plan

Source © Microsoft Learning 2015

Security Professionals and the Organization

- Wide range of professionals are required to support a diverse information security program.
- Senior management is the key component.
- Additional administrative support and technical expertise are required to implement details of the IS program.

Senior Management

- Chief information officer (CIO)
 - Senior technology officer
 - Primarily responsible for advising the senior executives on strategic planning
- Chief information security officer (CISO)
 - Has primary responsibility for assessment, management, and implementation of IS in the organization
 - Usually reports directly to the CIO

Information Security Project Team

- A small functional team of people who are experienced in one or multiple facets of required technical and nontechnical areas:
 - Champion
 - Team leader
 - Security policy developers
 - Risk assessment specialists
 - Security professionals
 - Systems administrators
 - End users

Data Responsibilities

- Data owners: senior management responsible for the security and use of a particular set of information
- Data custodians: responsible for the information and systems that process, transmit, and store it
- Data users: individuals with an information security role

Communities of Interest

- Group of individuals united by similar interests/values within an organization
 - Information security management and professionals
 - Information technology management and professionals
 - Organizational management and professionals

Information Security: Is It an Art or a Science?

- Implementation of information security is often described as a combination of art and science.
- “Security artisan” idea: based on the way individuals perceive system technologists and their abilities.

Security as Art

- No hard and fast rules nor many universally accepted complete solutions
- No manual for implementing security through entire system

Security as Science

- Dealing with technology designed for rigorous performance levels.
- Specific conditions cause virtually all actions in computer systems.
- Almost every fault, security hole, and systems malfunction is a result of interaction of specific hardware and software.
- If developers had sufficient time, they could resolve and eliminate faults.

Security as a Social Science

- Social science examines the behavior of individuals interacting with systems.
- Security begins and ends with the people that interact with the system, intentionally or otherwise.
- Security administrators can greatly reduce the levels of risk caused by end users and create more acceptable and supportable security profiles.

Summary (1 of 2)

- Computer security began immediately after the first mainframes were developed.
- Successful organizations have multiple layers of security in place: physical, personal, operations, communications, network, and information.
- Security should be considered a balance between protection and availability.

Summary (2 of 2)

- Information security must be managed similar to any major system implemented in an organization using a methodology like the SDLC.
- Implementation of information security is often described as a combination of art and science.