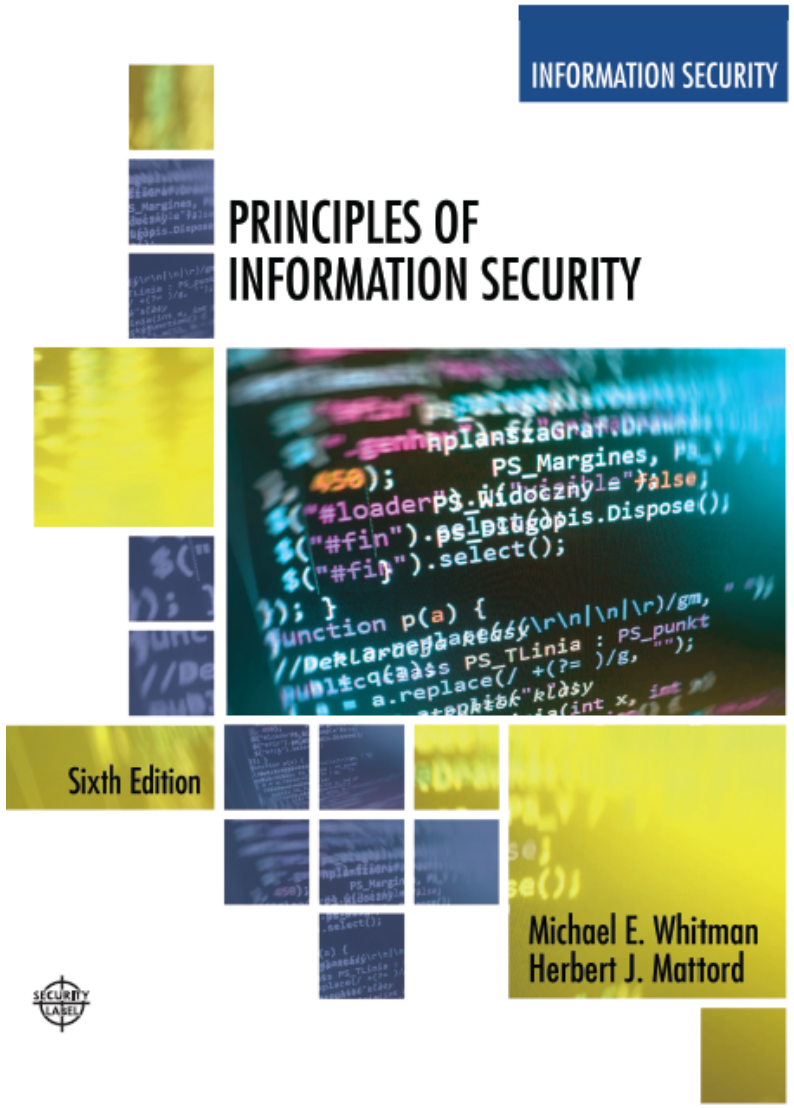


Source: Principles of Information Security

Chapter 1

Introduction to Information Security

Dr. Ibrahim Waziri Jr.

Learning Objectives

- 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

History of Information Security

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

Key Dates in Information Security

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. I 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.

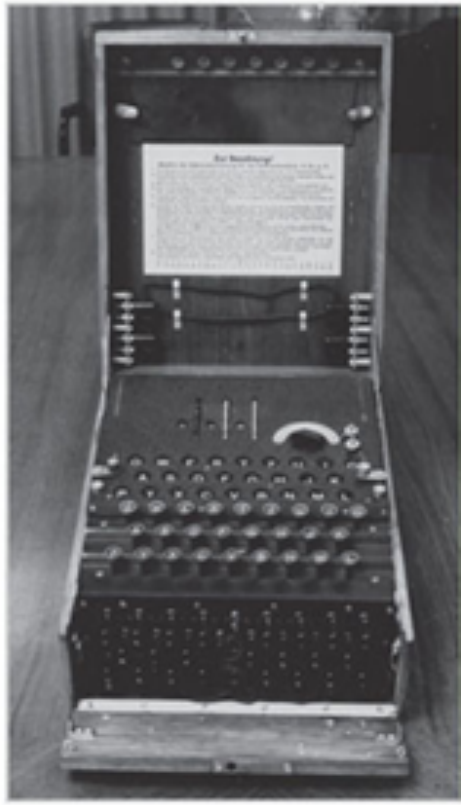
Table Reference: Principles of Information Security

Key Dates in Information Security (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.

Table Reference: Principles of Information Security

The Enigma



Source: Principles of Information Security

- An encryption device used by Germans for military communication during World War II
- 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. – Alan Turing
- The information gained from decrypted transmissions was used to anticipate the actions of German armed forces.

Resource: Watch The Imitation Game Movie

History of Computer Security

1960s

ARPANET Program

- ARPA now DARPA began researching redundant networked communications
- Larry Roberts developed the ARPANET from its inception.

1970s & 80s

Computer Security Begins!

- RAND Report R-609
- MULTICS Mainframe (First security-focused OS)
- Security scope grew from physical to data, access etc.

1970s & 80s Cont..

ARPANET Security Concerns

- No safety procedures for dial-up connections to ARPANET
- Non-existent user identification and authorization to system

80s & 1990s

Internet

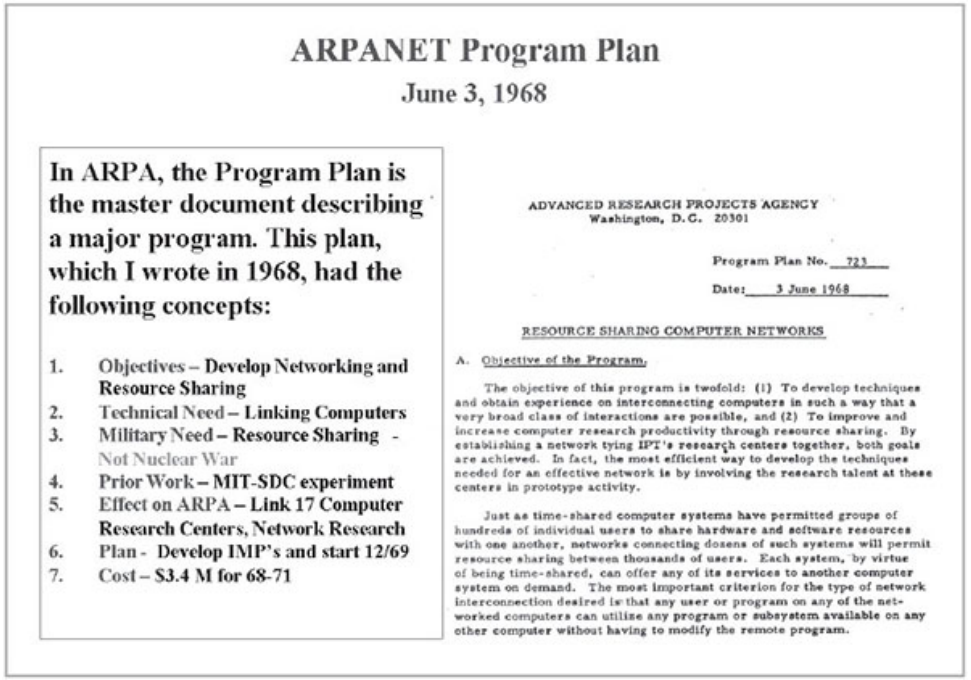
- Global Network of Networks (Unsecured/Low priority)
- DEFCON
- Morris Worm (First Virus)

2000s to present

Cyberattacks

- Millions of unsecured communications
- Dependency on networks
- Nation-states cyberwarfare
- Cyberterrorism

ARPANET Program Plan



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
6. Plan - Develop IMP's and start 12/69
7. Cost – $3.4 M for 68-71

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

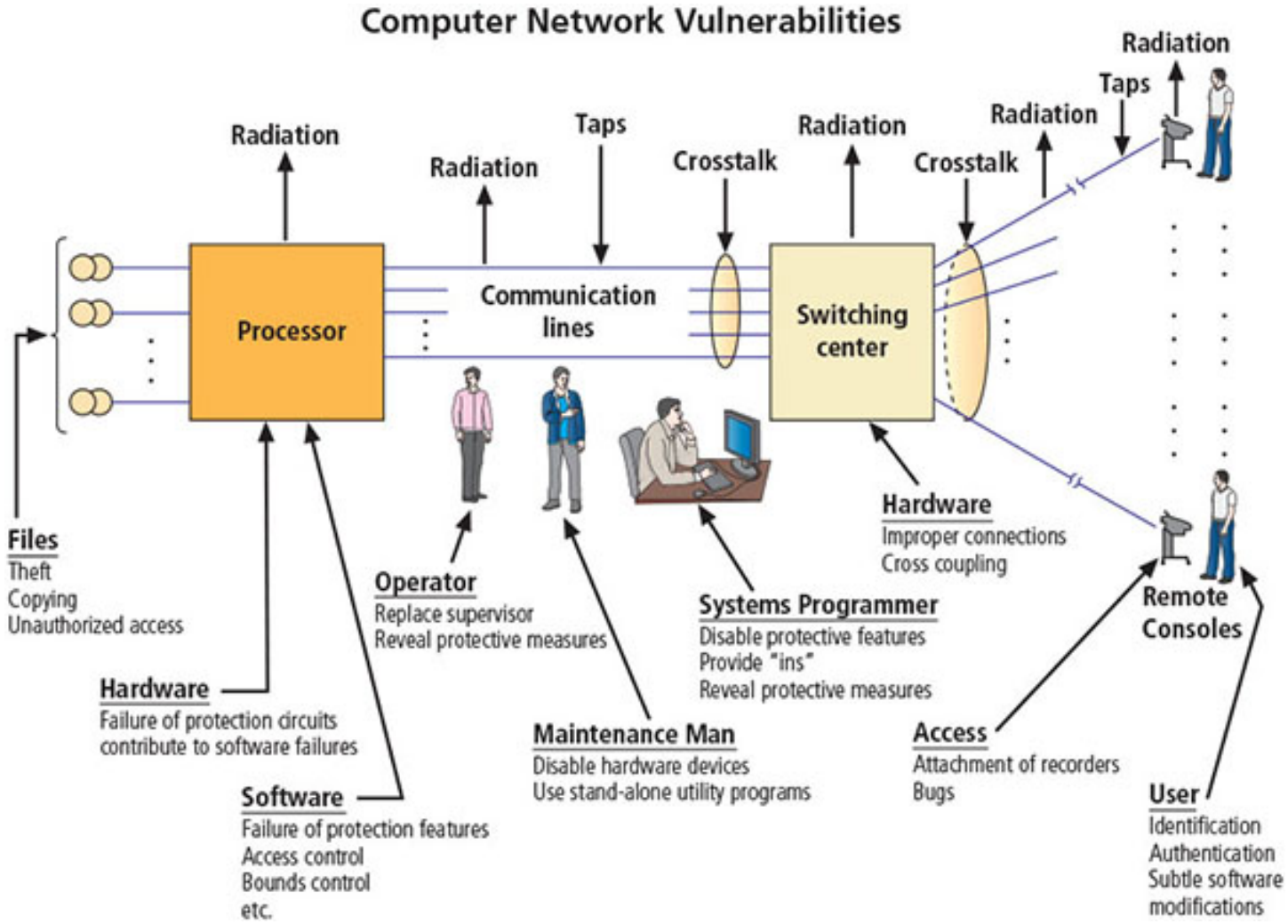
A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on 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 IPT'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 services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Source: Principles of Information Security

Network Vulnerability from RAND Report R-609



Source: Principles of Information Security

What is Security?

What is Security?

- A state of being secure and free from danger or harm; the actions taken to make someone or something secure.

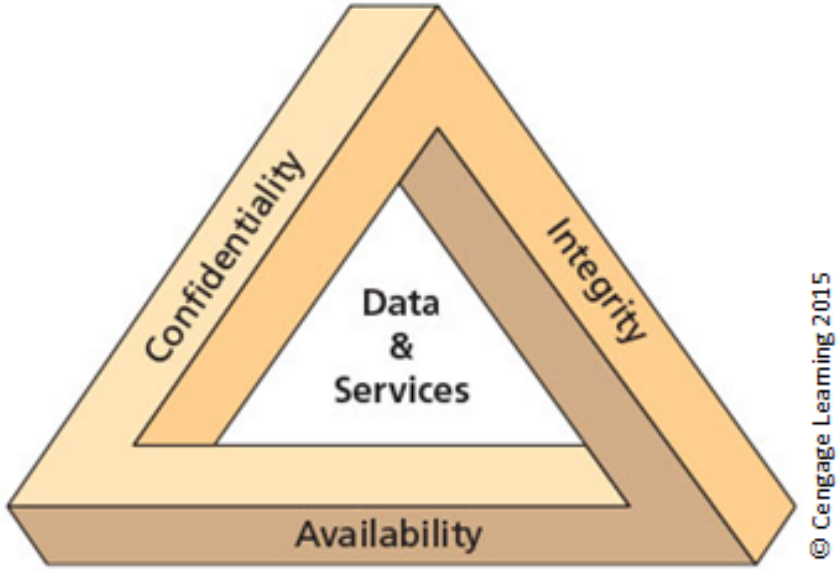
- Organizations should have multiple layers of security in place to protect its Operations, Physical infrastructure, People, Functions, Communications/Information etc.

Components of Information Security

Source: Principles of Information Security

- The protection of information and its critical elements:
  - Includes systems and hardware that use, store, and transmit that information
  - Includes information security management, data security, and network security

The CIA Triad



- Standard based on confidentiality, integrity, and availability.
- Now viewed as inadequate.

- Expanded model consists of a list of critical characteristics of information.

The value of information comes from the characteristics it possesses. Such as:

Availability, Accuracy, Authenticity, Confidentiality, Integrity, Utility, Possession

Source: Principles of Information Security

Key Information Security Concepts

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.

- Access
- Asset
- Attack
- Control, safeguard, or countermeasure
- Exploit
- Exposure
- Loss
- Protection profile or security posture
- Risk
- Subjects and objects of attack
- Threat
- Threat agent
- Threat event
- Threat source
- Vulnerability
- …etc

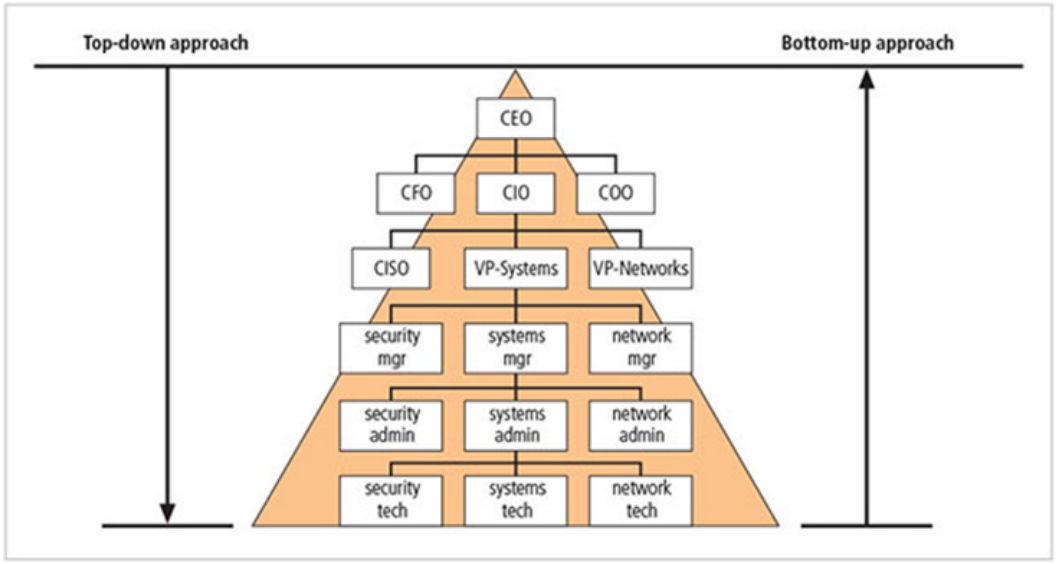
Resource: Refer to ISACA Glossary and ISC2 Cybersecurity Lexicon for a comprehensive information security phrases and definitions.

Components of an Information System

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

Implementing Information Security

Approaches to InfoSec Implementation



Source: Principles of Information Security

Bottom Up: Grassroots effort: Systems administrators attempt to improve security of their systems.

- Technical expertise of administrators
- Seldom works, as it lacks a number of critical features: Participant support, Organizational staying power.

Top Down: Initiated by upper management

- Issue policy, procedures, and processes
- Dictate goals and expected outcomes of project
- Determine accountability for each required action

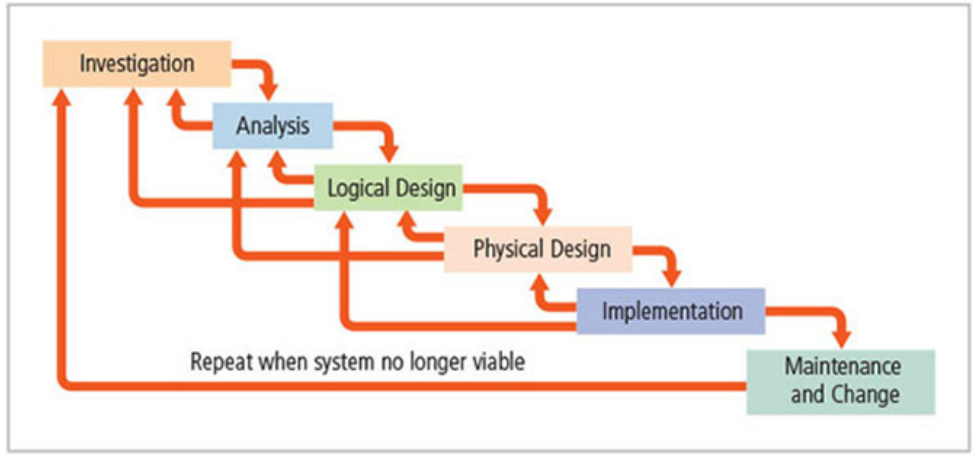
The most successful type of top-down approach also involves a formal development strategy referred to as systems development life cycle (SDLC).

Software/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



Source: Principles of Information Security

SDLC Stages:

- Investigation (Planning)
- Analysis
- Design (Logical and Physical)
- Implementation
- Maintenance (Operation/Change)
- Disposal

SDLC Deployment:

- Waterfall, Agile, DevOps, SecOps etc.

Resource: NIST 800-64 Rev 2 Document – "Security Considerations in the SDLC" outlines the methodology used to protect US Government Information Systems in compliance with FISMA of 2014

Security in SDLC: Software/Systems Assurance

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).

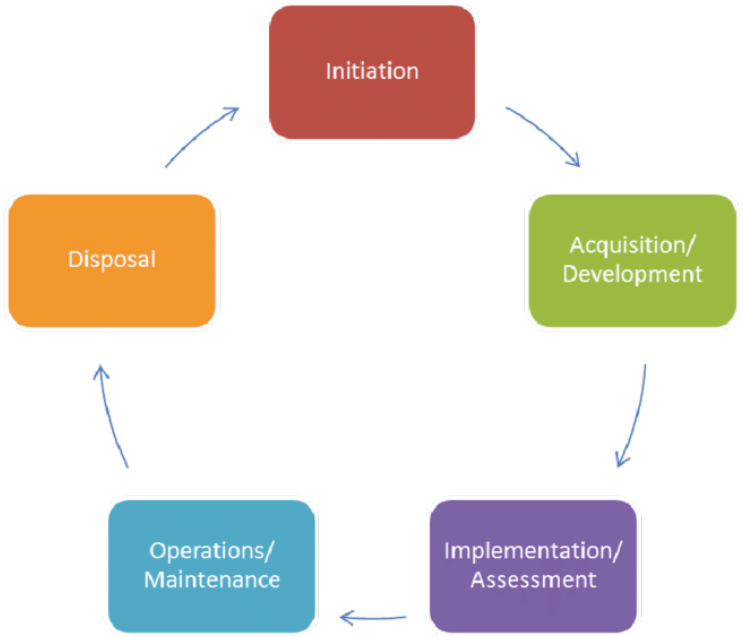
U.S. Department of Defense and Department of Homeland Security supported the Software Assurance Initiative, which resulted in the publication of Secure Software Assurance (SwA) Common Body of Knowledge (CBK).

SwA CBK serves as a strongly recommended guide to developing more secure applications.

Resource: Read "InfoSec/Privacy Considerations for Software in Advancing National Strategy to Secure Cyberspace" slide.

Security in SDLC: NIST approach

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

Source: NIST

Security in SDLC: Microsoft approach

Source: Microsoft

Security Professionals

Security Professionals & the Org.

- 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 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

Information Security: An Art or 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.

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

Chapter 1 Summary

Chapter Summary

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