INTRODUCTION TO INFORMATION SECURITY

INTRODUCTION

- James Anderson, executive consultant at Emagined Security, Inc., believes information security in an enterprise is a "well-informed sense of assurance that the information risks and controls are in balance." He is not alone in his perspective.
- Many information security practitioners recognize that aligning information security needs with business objectives must be the top priority.

History of Information Security

- The history of information security begins with the history of computer security. The need for computer security that is need to secure physical locations, hardware, and software from outside threats- arose during World War II when the first mainframes, developed to aid computations for communication code breaking.
- Multiple levels of security were implemented to protect these mainframes and secure data integrity. Access to sensitive military locations, for example, was controlled through the use of badges, keys, and facial recognition of authorized personnel by security guards.
- The growing need to maintain national security eventually led to more complex and more technologically sophisticated computer security safeguards.

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."

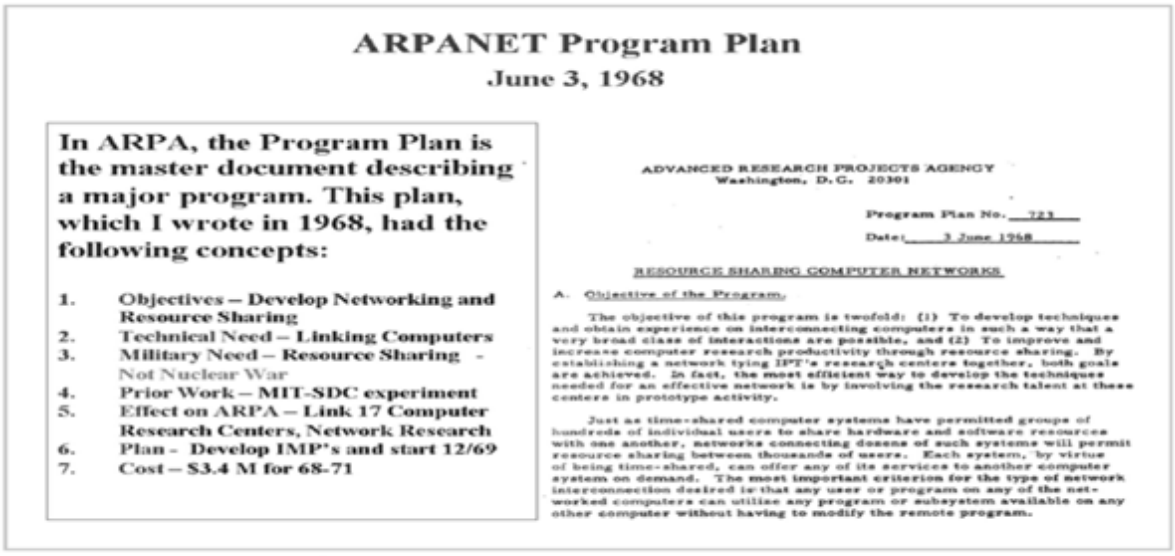
Courtesy of National Security Agency

The Enigma[2]

- During these early years, information security was a straight forward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage.
- One of the first documented security problems that was not physical in nature occurred in the early 1960's, when a systems administrator was working on a MOTD (message of the day) file, and another administrator was editing the password file.
- A software glitch mixed the two files, and the entire password file was printed on every output file.

The 1960's

- During the cold war, many more mainframes were brought online to accomplish more complex and sophisticated tasks. It became necessary to find a way to enable these mainframes to communicate with each by means of a less cumbersome process than mailing magnetic tapes between computer centers.



ARPANET Program Plan[4]

- In response to this need, the Department of defense's Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military's exchange of information.
- Larry Roberts, known as the founder of the internet, developed the project from its inception stage. This project, called ARPANET, is the origin of today's internet.

The 1970s and 80s

- During the next decade, the ARPANET became popular and more widely used, and the potential for its misuse grew. In December of 1993, Robert M. "BOB" who is credited with the development of the Ethernet, one of the most popular networking protocols, identified fundamental problems with ARPANET security.

Problems of ARPANET

- Individual remote user's sites did not have sufficient controls and safeguards to protect data from unauthorized remote users.
- Vulnerability of password structure and formats
- Lack of security procedures for dial up connections

The Rand report R 609 was the first widely recognized published document to identify the role of management and policy issues in computer security. It noted that the wide utilization of networking components in information systems in the military introduced security risks that could not be mitigated by the routine practices then used to secure these systems.

When the scope of computer security expanded significantly from the safety of physical locations and hardware to include the following:

- Securing the data
- Limiting random and unauthorized access to that data
- Involving personnel from multiple levels of the organization in matter pertaining to information security.

Multics

- Much of the early focus for research on computer security centered on a system called Multiplexed Information and computing service (MULTICS). Although this operating system is now obsolete. MULTICS is noteworthy because it was the first operating system created with security as its primary goal.
- It was a mainframe, time sharing operating system developed in the mid 1960's by a consortium of general electric Bell Labs, and the Massachusetts institute of Technology (MIT).

- In mid-1969 not long after the restructuring of the MULTICS project, several of its key players (Ken Thompson, Dennis Ritchie, Rudd Canaday, and Doug Mcilro) created a new operating system called UNIX. While the MULTICS system implemented multiple security levels and passwords, the UNIX system did not.

The 1990s

- At the close of the twentieth century, networks of computers became more common, as did the need to connect these networks to each other. This gave rise to the internet, the first global network of networks, this networking resource was made available to the general public in the 1990's, having previously been the domain of government, academia, and dedicated industry professionals.
- The internet brought connectivity to virtually all computers that could reach a phone line or an internet connected local area network (LAN). After the internet was commercialized, the technology became pervasive, reaching almost every corner of the globe with an expanding array of uses.

1.1 WHAT IS SECURITY?

- Understanding the technical aspects of information security requires that you know the definitions of certain information technology terms and concepts. In general, security is defined as "the quality or state of being secure—to be free from danger." In other words, protections against adversaries from those who would do harm, intentionally or otherwise- is the objective.

- Security is often achieved by means of several strategies usually undertaken simultaneously or used in combination with one another.

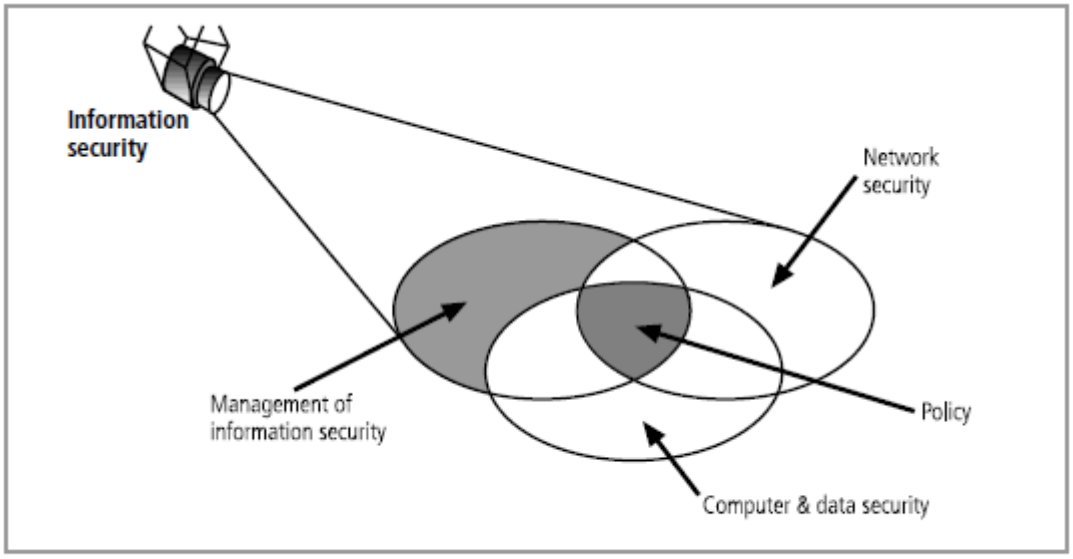
A successful organization should have the following multiple layers of security in place to protect its operations.

- **Physical security,** which encompasses strategies to protect people, physical assets, and the workplace from various threats including fire, unauthorized access, or natural disasters.
- **Personal security,** which overlaps with physical security in the protection of the people within the organization.
- **Operations security**, which focuses on securing the organization's ability to carry out its operational activities without interruption or compromise.

- **Communications security**, which encompasses the protection of an organization's communications media, technology, and content, and its ability to use these tools to achieve the organization's objectives.
- **Network security**, which addresses the protection of an organization's data networking devices, connections, and contents, and the ability to use that network to accomplish the organization's data communication functions.
- **Information security** includes the broad areas of information security management, computer and data security, and network security.

Where it has been used?

- Governments, military, financial institutions, hospitals, and private businesses.
- Protecting confidential information is a business requirement.



Components of Information Security

1.1.1 Information Security components:

- The C.I.A triangle has been the industry standard for computer security since the development of the mainframe.
- To protect information and its related systems, organizations must implement such tools as policy, awareness, training and education, and technology. The NSTISSC model of information security evolved from a concept developed by the computer security industry known as the C.I.A triangle.

- Confidentiality
- Integrity
- Availability

- Information security (InfoSec) as defined by the standards published by the committee on National security Systems (CNSS), formerly the National security Telecommunications and information systems security committee (NSTISSC).
- It is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

CIA Triangle

- The C.I.A. triangle - confidentiality, integrity, and availability - has expanded into a more comprehensive list of critical characteristics of information. The security of these three characteristics of information is as important today as it has always been, but the C.I.A triangle model no longer adequately addresses the constantly changing environment of the computer industry.

CIA Triangle

- The threats to information confidentiality, integrity, and availability have evolved into a vast collection of events, including accidental or intentional damage, destruction, theft, unintended or unauthorized modifications, or other misuses from human or nonhuman threats.

1.2 CRITICAL CHARACTERISTICS OF INFORMATION

The value of information comes from the characteristics it possesses. When a characteristic of information changes, the value of that information either increases, or more commonly decreases. Some characteristics affect information's value to users more than others do. This can depend on circumstances; For example timeliness of information can be critical factor, because information loses much or all of its value when it is delivered late.

The following are some of the characteristics of information.

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility
- Possession

1.2.1 Availability

- Availability is the characteristic of information that enables user access to information without interference or obstruction and in a required format. A user in this definition may be either a person or another computer system. Availability does not imply that the information is accessible to any user; rather, it means availability to authorized users.
    - For any information system to serve its purpose, the information must be available when it is needed.
    - Eg: High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.

Privacy

- The information that is collected, used, and stored by an organization is to be used only for the purposes stated to the data owner at the time it was collected. This definition of privacy does focus on freedom from observation (the meaning usually associated with the word), but rather means that information will be used only in ways known to the person providing it.

Identification

- An information system possesses the characteristic of identification when it is able to recognize individual users. Identification and authentication are essential to establishing the level of access or authorization that an individual is granted.

Authentication

- Authentication occurs when a control provides proof that a user possesses the identity that he or she claims.
- In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine (i.e. they have not been forged or fabricated)

Authorization

- After the identity of a user is authenticated, a process called authorization provides assurance that the user (whether a person or a computer) has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset.

Accountability

- The characteristic of accountability exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process. For example, audit logs that track user activity on an information system provide accountability.

1.2.2 Confidentiality

Confidentiality of information ensures that only those with sufficient privileges may access certain information. When unauthorized individuals or systems can access information, confidentiality is breached. To protect the confidentiality of information, a number of measures are used:

- Information classification
- Secure document storage
- Application of general security policies
- Education of information custodians and end users. Example, a credit card transaction on the Internet.

- The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in data bases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored.

- Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information, it could result in a breach of confidentiality.

Integrity

- Integrity is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being compiled, stored, or transmitted.
- Integrity means that data cannot be modified without authorization.
  Eg: Integrity is violated when an employee deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a website, when someone is able to cast a very large number of votes in an online poll, and so on.

1.2.3 Accuracy

Information should have accuracy. Information has accuracy when it is free from mistakes or errors and it has the value that the end users expects. If information contains a value different from the user's expectations, due to the intentional or unintentional modification of its content, it is no longer accurate.

Utility

- Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end user, it is not useful. Thus, the value of information depends on its utility.

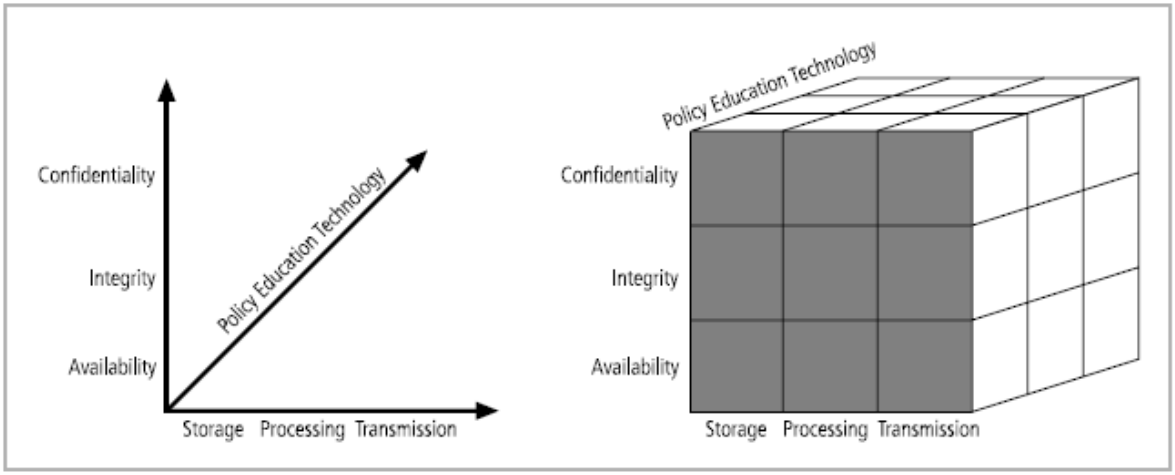
Possession

- The possession of Information security is the quality or state of having ownership or control of some object or item.

1.3 NSTISSC SECURITY MODEL

'National Security Telecommunications & Information systems security committee' document.

- It is now called the National Training Standard for Information security professionals.
- The NSTISSC Security Model provides a more detailed perspective on security.
- While the NSTISSC model covers the three dimensions of information security, it omits discussion of detailed guidelines and policies that direct the implementation of controls.



NSTISSC Security Model

Another weakness of using this model with too limited an approach is to view it from a single perspective.

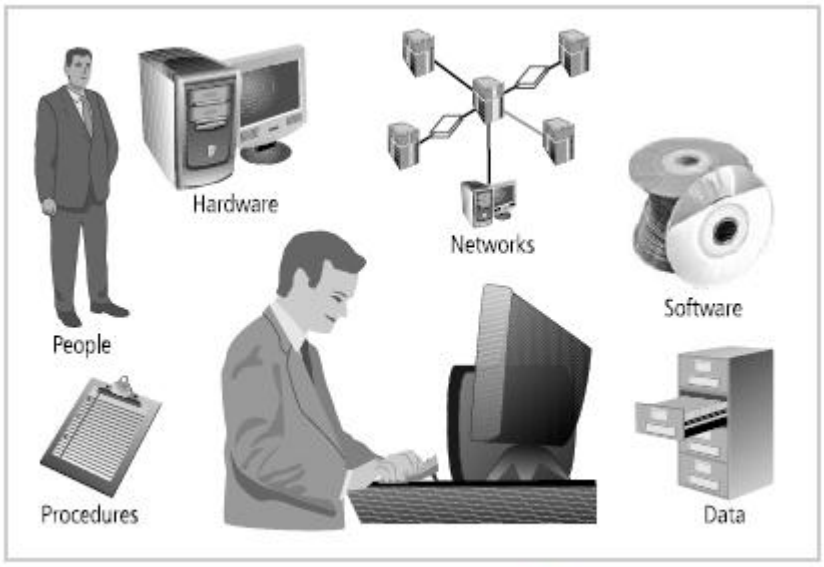
- The 3 dimensions of each axis become a 3x3x3 cube with 27 cells representing areas that must be addressed to secure today's Information systems.
- To ensure system security, each of the 27 cells must be properly addressed during the security process.
- For example, the intersection between technology, integrity, and storage requires a control or safeguard that addresses the need to use technology to protect the integrity of information while in storage. One such control might be a system for detecting host intrusion that protects the integrity of information by alerting the security administrators to the potential modification of a critical file. What is commonly left out of such a model is the need for guidelines and policies that provide direction for the practices and implementations of technologies. The need for policy is discussed in subsequent chapters of this book.

1.4 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.

- Software
- Hardware
- Data
- People
- Procedures
- Networks

These six critical components enable information to be input, processed, output, and stored. Each of these IS components has its own strengths and weakness-its own characteristics and uses. More important to remember, each component of the information systems has its own security requirements.



Components of an Information System

1.4.1 Software

- The software components of IS comprises applications, operating systems, and assorted command utilities.
- Software is perhaps the most difficult IS component to secure.
- The Exploitation of errors in software programming accounts for a substantial portion of the attacks on information.

- Software programs are the vessels that carry the lifeblood of information through an organization. These are often created under the demanding constraints of project management, which limit time, cost, and manpower.

1.4.2 Hardware

- Hardware is the physical technology that houses and executes the software, stores and carries the data, and provides interfaces for the entry and removal of information from the system.
- Physical security policies deal with hardware as a physical asset and with the protection of these physical assets from harm or theft. Applying the traditional tools of physical security, such as locks and keys, restricts access to and interaction with the hardware components of an information system.
- Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information. Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted access to the hardware is possible.

1.4.3 Data

- Data stored, processed, and transmitted through a computer system must be protected.
- Data is often the most valuable asset possessed by an organization and is the main target of intentional attacks.
- Systems developed in recent years are likely to have been created to make use of database management systems.
- The raw, unorganized, discrete (separate, isolated) potentially-useful facts and figures that are later processed (manipulated) to produce information.

1.4.4 People

- The people can the weakest link in an organization's information security program. Though often overlooked in computer security considerations, people have always been a threat to information security.
- And unless policy, education and training, awareness, and technology are properly employed to prevent people from accidentally or intentionally damaging or losing information, they will remain the weakest link.
- There are many roles for people in information systems. Common ones include
    - Systems Analyst

- Programmer
- Technician
- Engineer
- Network Manager
- MIS (Manager of Information Systems)
- Data entry operator

1.4.5 Procedures

- Procedures are written instructions accomplishing a specific task. When an unauthorized user obtains an organization's procedures, this poses a threat to the integrity of the information.
- A procedure is a series of documented actions taken to achieve something. A procedure is more than a single simple task. A procedure can be quite complex and involved, such as performing a backup, shutting down a system, patching software.
- Educating employees about safeguarding the procedures is as important as securing the information system. Therefore knowledge of procedures as with all critical information should be disseminated among members of the organization only on a need to know basis.

1.4.6 Networks

- When information systems are connected to each other to form Local Area Network (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.
- Applying the traditional tools of physical security, such as locks and keys, to restrict access to and interaction with the hardware components of an information system are still important.
- Steps to provide network security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

1.5 SECURING COMPONENTS

- The security of information and its systems requires that you secure and protect all components from misuse and abuse by unauthorized users.
- It is important to understand that a computer can be either the Subject or Object of an attack.
    - Subject of an attack

      Computer is used as an active tool to conduct the attack.

- Object of an attack

  Computer itself is the entity being attacked

Two types of attacks:

- Direct attack
- Indirect attack

Direct attack

- When a Hacker uses his personal computer to break into a system.[Originate from the threat itself]

Indirect attack

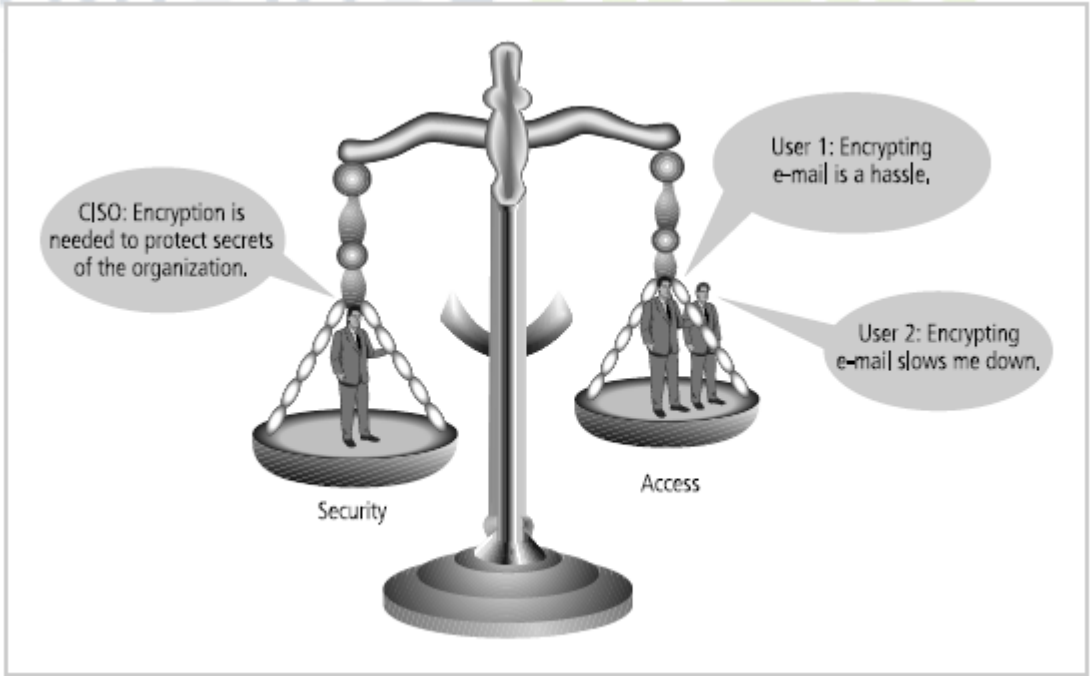
- When a system is compromised and used to attack other system.
- [Originate from a system or resource that itself has been attacked, and is malfunctioning or working under the control of a threat].

A computer can, therefore, be both the subject and object of an attack when, for example, it is first the object of an attack and then compromised and used to attack other systems, at which point it becomes the subject of an attack.

1.6 BALANCING INFORMATION SECURITY AND ACCESS

- Even with the best planning and implementation, it is impossible to obtain perfect information security. Recall James Anderson's statement, which emphasizes the need to balance security and access.
- Information security cannot be absolute: it is a process, not a goal. It is possible to make a system available to anyone, anywhere, anytime, through any means. However, such unrestricted access poses a danger to the security of the information.
- On the other hand, a completely secure information system would not allow anyone access. For instance, when challenged to achieve a TCSEC C-2 level security certification for its Windows operating system, Microsoft had to remove all networking components and operate the computer from only the console in a secured room.

- To achieve balance—that is, to operate an information system that satisfies the user and the security professional—the security level must allow reasonable access, yet protect against threats.



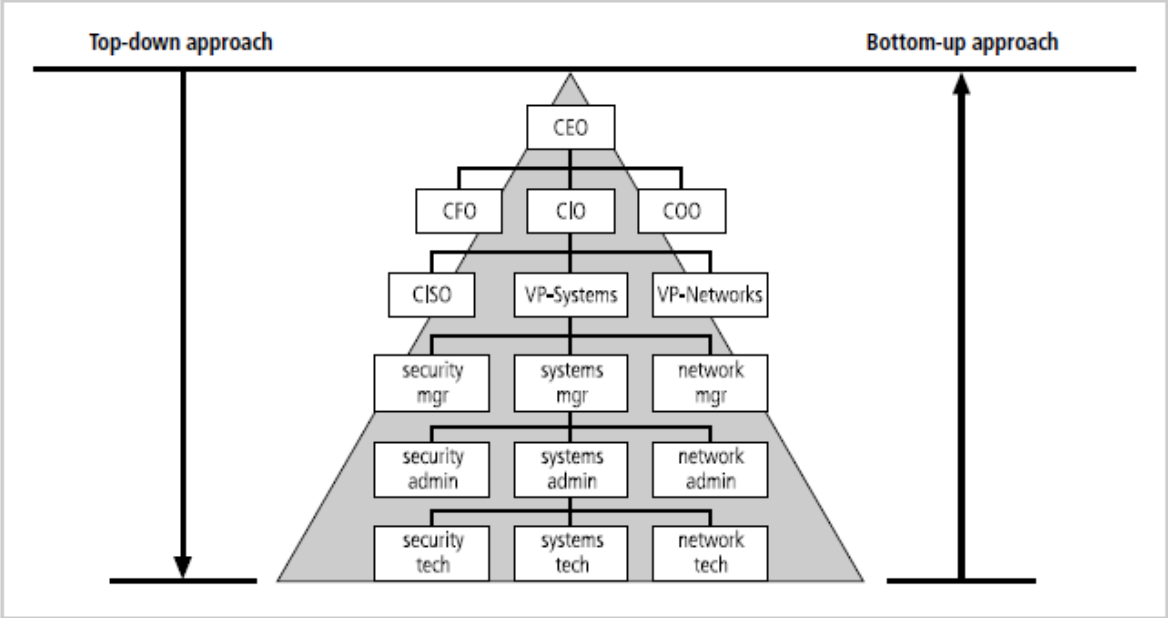
Balancing Information Security and Access

- Information system or data-processing department can get too entrenched in the management and protection of systems. An imbalance can occur when the needs of the end user are undermined by too heavy a focus on protecting and administering the information systems.
- Both information security technologists and end users must recognize that both groups share the same overall goals of the organization—to ensure the data is available when, where, and how it is needed, with minimal delays or obstacles.
- In an ideal world, this level of availability can be met even after concerns about loss, damage, interception, or destruction have been addressed.

1.6.1 Approaches to Information Security Implementation

- The implementation of information security in an organization must begin somewhere, and cannot happen overnight.
- There are two types of implementation,
  - Bottom-up approach

- Top-down approach



Approaches to Information Security Implementation

Bottom-up approach

- Securing information assets is in fact an incremental process that requires coordination, time, and patience. Information security can begin as a grassroots effort in which systems administrators attempt to improve the security of their systems. This is often referred to as a bottom-up approach.
- The key advantage of the bottom-up approach is the technical expertise of the individual administrators. Working with information systems on a day-to-day basis, these administrators possess in-depth knowledge that can greatly enhance the development of an information security system. They know and understand the threats to their systems and the mechanisms needed to protect them successfully.
- Unfortunately, this approach seldom works, as it lacks a number of critical features, such as participant support and organizational staying power.

Top-down approach

- The top-down approach—in which the project is initiated by upper-level managers who issue policy, procedures and processes, dictate the goals and expected outcomes, and determine accountability for each required action—has a higher probability of success.

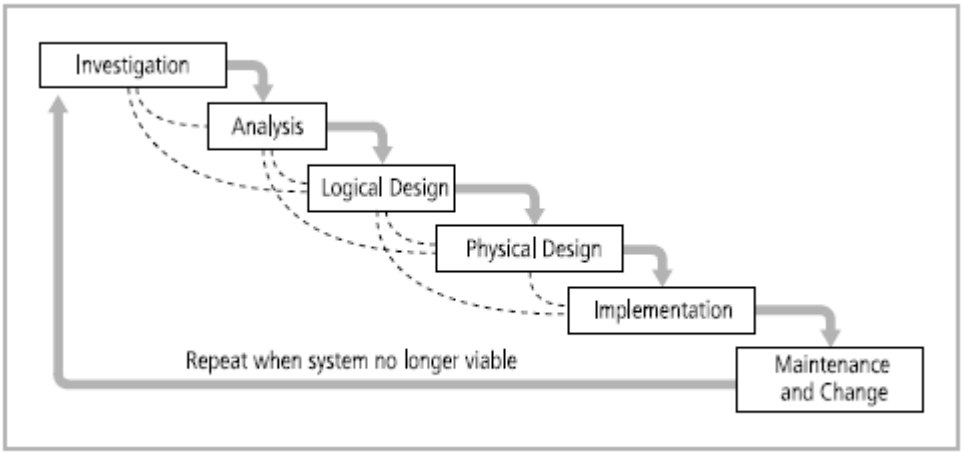
- This approach has strong upper-management support, a dedicated champion, usually dedicated funding, a clear planning and implementation process, and the means of influencing organizational culture.
- The most successful kind of top-down approach also involves a formal development strategy referred to as a systems development life cycle.

1.7 SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

- The information security must be managed in a manner similar to any other major system implemented in an organization.
- One approach for implementing an information security system in an organization with little or no formal security in a place is to use a variation of the systems development life cycle (SDLC): the security systems development life cycle (SecSDLC).

1.7.1 Methodology and Phases

- The systems development life cycle (SDLC) is a methodology for the design and implementation of an information system. A methodology is a formal approach to solving a problem by means of a structured sequence of procedures.
- Using a methodology ensures a rigorous process with a clearly defined goal and increases the probability of success.
- The traditional SDLC consists of six general phases. If you have taken a system analysis and design course, you may have been exposed to a model consisting of a different number of phases. SDLC models range from having three to twelve phases, all of which have been mapped into the six presented here.
- The waterfall model pictured in Figure, illustrates that each phase begins with the results and information gained from the previous phase.
- At the end of each phase comes a structured review or reality check, during which the team determines if the project should be continued, discontinued, outsourced, postponed, or returned to an earlier phase depending on whether the project is proceeding as expected and on the need for additional expertise, organizational knowledge, or other resources.



SDLC Waterfall Methodology

- Once the system is implemented, it is maintained (and modified) over the remainder of its operational life.

Investigation

- The first phase, investigation, is the most important. What problem is the system being developed to solve?
- It is the most important phase and it begins with an examination of the event or plan that initiates the process.
- During this phase, the objectives, constraints, and scope of the project are specified.
- At the conclusion of this phase, a feasibility analysis is performed, which assesses the economic, technical and behavioural feasibilities of the process and ensures that implementation is worth the organization's time and effort.

Analysis

- It begins with the information gained during the investigation phase.
- It consists of assessments (quality) of the organization, the status of current systems, and the capability to support the proposed systems.
- Analysts begin by determining what the new system is expected to do, and how it will interact with existing systems.
- This phase ends with the documentation of the findings and an update of the feasibility analysis.

Logical Design

- In this phase, the information gained from the analysis phase is used to begin creating a systems solution for a business problem.

- Based on the business need, applications are selected that are capable of providing needed services.
- Based on the applications needed, data support and structures capable of providing the needed inputs are then chosen.
- In this phase, analysts generate a number of alternative solutions, each with corresponding strengths and weaknesses, and costs and benefits.
- At the end of this phase, another feasibility analysis is performed.

Physical design

- In this phase, specific technologies are selected to support the solutions developed in the logical design.
- The selected components are evaluated based on a make-or-buy decision.
- Final designs integrate various components and technologies.

Implementation

- In this phase, any needed software is created.
- Components are ordered, received and tested.
- Afterwards, users are trained and supporting documentation created.
- Once all the components are tested individually, they are installed and tested as a system.
- Again a feasibility analysis is prepared, and the sponsors are then presented with the system for a performance review and acceptance test.

Maintenance and change

- It is the longest and most expensive phase of the process.
- It consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle.
- Periodically, the system is tested for compliance, with business needs.
- Upgrades, updates, and patches are managed.
- As the needs of the organization change, the systems that support the organization must also change.
- When a current system can no longer support the organization, the project is terminated and a new project is implemented.

Securing the SDLC

- Each of the phases of the SDLC should include consideration of the security of the system being assembled as well as the information it uses.
- Whether the system is custom and built from scratch, is purchased and then customized, or is commercial off-the-shelf software (COTS), the implementing organization is responsible for ensuring it is used securely.

1.8 SECURITY SYSTEMS DEVELOPMENT LIFE CYCLE (SEC SDLC)

- The same phases used in the traditional SDLC can be adapted to support the implementation of an information security project. While the two processes may differ in intent and specific activities, the overall methodology is the same.
- At its heart, implementing information security involves identifying specific threats and creating specific controls to counter those threats. The SecSDLC unifies this process and makes it a coherent program rather than a series of random, seemingly unconnected actions.

1.8.1 Sec SDLC phases

Investigation

- This phase begins with a directive from upper management, dictating the process, outcomes, and goals of the project, as well as its budget and other constraints.
- Frequently, this phase begins with an enterprise information security policy, which outlines the implementation of a security program within the organization.
- Teams of responsible managers, employees, and contractors are organized.
- Problems are analyzed.
- Scope of the project, as well as specific goals and objectives, and any additional constraints not covered in the program policy, are defined.
- Finally, an organizational feasibility analysis is performed to determine whether the organization has the resources and commitment necessary to conduct a successful security analysis and design.

Analysis

- In this phase, the documents from the investigation phase are studied.

- The developed team conducts a preliminary analysis of existing security policies or programs, along with that of documented current threats and associated controls.
- The risk management task also begins in this phase.
- Risk management is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security and to the information stored and processed by the organization.

Logical design

- This phase creates and develops the blueprints for information security, and examines and implements key policies.
- The team plans the incident response actions.
- Plans business response to disaster.
- Determines feasibility of continuing and outsourcing the project.
- The planning answers the following questions.
- Continuity planning: How will business continue in the event of a loss?
- Incident response: What steps are taken when an attack occurs?
- Disaster recovery: What must be done to recover information and vital systems immediately after a disastrous event?

Physical design

- In this phase, the information security technology needed to support the blueprint outlined in the logical design is evaluated.
- Alternative solutions are generated.
- Designs for physical security measures to support the proposed technological solutions are created.
- At the end of this phase, a feasibility study should determine the readiness of the organization for the proposed project.
- At this phase, all parties involved have a chance to approve the project before implementation begins.

Implementation

- The implementation phase in of SecSDLC is also similar to traditional SDLC.
- The security solutions are acquired (made or bought), tested, implemented, and tested again

- Personnel issues are evaluated and specific training and education programs are conducted.
- Finally, the entire tested package is presented to upper management for final approval.
- The implementation phase requires the following things.
    - Inspection and Acceptance
    - System integration
    - Security certification
- Security accreditation

Maintenance and change

- Constant monitoring, testing, modification, updating, and repairing to meet changing threats have been done in this phase.

1.9 SECURITY PROFESSIONALS AND THE ORGANIZATION

- It takes a wide range of professionals to support a diverse information security program. Senior management is the key component and the vital force for a successful implementation of an information security program.
- But administrative support is also essential to developing and executing specific security policies and procedures, and technical expertise is of course essential to implementing the details of the information security program.

Senior management

Chief information Officer (CIO) is the responsible for

- Assessment
- Management
- And implementation of information security in the organization

Information Security Project Team

- Champion
    - Promotes the project
    - Ensures its support, both financially & administratively.
- Team Leader
    - Understands project management
    - Personnel management
    - And information Security technical requirements.

- Security policy developers
  - Individuals who understand the organizational culture,
  - Existing policies
  - Requirements for developing & implementing successful policies.
- Risk assessment specialists
  - Individuals who understand financial risk assessment techniques.
  - The value of organizational assets, and the security methods to be used.
- Security Professionals
  - Dedicated
  - Trained, and well educated specialists in all aspects of information security from both a technical and non-technical stand point.
- System Administrators
  - Administrating the systems that house the information used by the organization.
- End users
  - Ideally, a selection of users from various departments, levels, and degrees of technical knowledge assist the team in focusing on the application of realistic controls applied in ways that do not disrupt the essential business activities they seek to safeguard.

Data Responsibilities

The three types of data ownership and their respective responsibilities are,

- Data Owners
  - Responsible for the security and use of a particular set of information.
  - Determine the level of data classification
  - Work with subordinate managers to oversee the day-to-day administration of the data.
- Data Custodians
  - Responsible for the storage, maintenance, and protection of the information.
  - Overseeing data storage and backups
  - Implementing the specific procedures and policies.
- Data Users (End users)
  - Work with the information to perform their daily jobs supporting the mission of the organization. Everyone in the organization is responsible for the security of data, so data users are included here as individuals with an information security role.